Basic Computer Security:
Basic Internet tips

Which browser to use?

Not all browsers are made equal, but all work in essentially the same way. There's no wrong answer to this question but when it comes to safety and privacy you have choices.

Chrome is known for its security but you may be trading off a bit of privacy.

Firefox is the next step below Chrome on security and offers good privacy while browsing.

Internet Explorer is the least secure of the three and offers okay privacy while browsing.

How do I know if a website is safe?

Websites now use certificates that communicate with your web browser to let them know how safe and secure they are. Many sites will now feature an icon next to the url in the address bar. Most browsers will now also warn you when you click to go to a site that seems unsafe.

What's a strong password?

A strong password is one that is hard to guess, is a mix of letters/numbers/symbols, and only associated with one log-in.

Why should I not use the same password multiple places?

The reason it is important to use multiple passwords is that if someone is able to get one of your passwords they are not able to log in to every service you use. If your online bank password was the same as your email password and someone hacked your email you'd be in a lot of trouble!

How can I possibly remember all my different passwords!?

This is the downside to both strong passwords and following the rule of having a unique password for every log-in. But rest assured you're not alone in this struggle. Many people take to keeping a notebook or folder where they write all their passwords down. While this will help you when you need to look up a password it's not very safe. If you were to ever lose that book/folder you'd have no way to get your passwords back and if someone stole it they would have every single password you've ever written down. So how about at this point we offer some tips and solutions!

There are many services online that offer a free way to securely store your passwords. It's the same as having a notebook but now you have a company protecting that notebook and you can access it anywhere you get on the internet. Some services offer apps for your phone or tablet for a small fee. These services usually include features that will create secure passwords for you. Lastly you'll need a password to get into your online password notebook/vault. This would be your "master password."

Lifehacker.com – "Lifehacker Faceoff: The Best Password Mangers, Compared"

http://lifehacker.com/lifehacker-faceoff-the-best-password-managers-compare-1682443320

Tips on making a good master password:

Mnemonics! You may have forgotten this term but you've more than likely used mnemonics to remember things for school. Mnemonics is creating a phrase that helps you remember something else. A famous one is "Please Excuse My Dear Aunt Sally" which is used in math to remember the order of problem solving (P- Parentheses E- Exponents M- Multiple D- Divide A- Add S- Subtract). Mnemonics really help to remember a random string of letters and numbers which make a strong master password. Example:

u3bRH65

Could become the phrase: "yo**u 3 b**etter **R**emember **H**alftime **65**"

The phrase doesn't make a lot of sense, but that can help you to remember it. The more you say it to yourself the more you'll remember it. Soon when you go to log in you'll find yourself thinking "you 3 better Remember Halftime 65" as you type out your password. Additionally because this is random and a meaningless phrase even if you said it out loud no one would know which parts of the words/numbers are important and make up the password you're typing. For example it's the U in you but the B in better, one is the last letter and the other is the first. The important thing is that you remember. Practice logging in and out with the password while reciting the phrase in your mind. This will also help with muscle memory as your hands will get used to typing the password.

What to do about those security questions?

Ironically security questions make you less secure! Many websites are moving away from them because when answered correctly they tend to be easy to figure out. If you answer what is your mother's maiden name someone might find that out using what's called "Social Engineering." Social engineering is a practice where people use conversations and questions to learn valuable information that might be used for security questions. Have you ever reminisced about your first car? That's a pretty common security question. So how can you protect yourself when a site requires you to use security questions?

One possible solution is that you act like a secret agent and you trick the system. The answers for the questions do not have to be correct, they just have to be what you want them to be. A good trick is to pick 6 common security questions and then match them into pairs. For example pick "What is your mother's maiden name?" and match it to "What city were you born in?" Now use one question to answer the other! No company cares if you say your mother's maiden name is Lacrosse, nor would they care if you said you were born in Anderson. What's important is that you remember which questions you switched around. Or if you want to be really safe you can use your password keeper and where you save your password you can save your security questions and make the answers completely random. As long as you remember your one important master password you'll have access to all your other log-in information.

Another solution is to pick one set of security questions and make up a fake answer for each one that you can remember. Again they don't need to make sense. If you want to say your first car was "a fish" the computer won't mind but no one will be able to figure out that answer just by having a normal

conversation with you.

What is catfishing?

Catfishing uses social engineering but done online and over a longer duration. People will make fake profiles on social media websites and create a full life for this fake individual. Once the person has established the fake profile they'll then start using that profile to contact strangers. Using these profiles the scam artists will start to try to social engineer information or make pleas for money or gifts.

The best way to protect yourself from catfishing is to already be following the method of having a secure password and security questions that can't be answered simply by knowing a few things about you. Additionally on social media if something sounds too good to be true it most likely is. While it would be great if a Nigerian prince was really giving out free money when you shared your banking information it's just not likely to happen.

Email documents, should I open them?

If you don't know the person or company the email is being sent from then it's best not to open or download that file. Most web browsers and antivirus software will scan files before, during, or after they're downloaded but nothing is foolproof so you're always better off taking the side of caution.

Internet settings

What is incognito/private browsing? What it does and does not do for you.

Incognito/InPrivate/Private mode (Chrome/IE/Firefox in order) is a way to browse the internet but the name is misleading. What we think is private is different than what others think is private. What these modes actually do is prevent your browser from collecting and storing cookies, site visit history, and saved information your browser might otherwise store on your computer. What these modes don't do is protect you from the outside world. If you're at work for example and you're in these modes your company can still see what websites you're visiting. This is not a 'safer' way to browse, it's a way to not have your computer store whatever you did in the last time you used the internet.

What the heck is a cache and what are cookies?

Your computer wants to work smarter and not harder, so behind the scenes your computer is doing many different things you never actually see for yourself. In particular when it comes to the internet your computer wants to load websites as quickly as possible for you. This is where cache and cookies become important. Your cache is storage on your computer dedicated to files from websites, particularly images or anything that would slow loading a website. By allowing your cache to store these your computer does not have to download them each time you visit a website, thus saving you time when the page loads.

Cookies are the text files stored in the cache that keep all that information that your computer will load. What's important to know is that when you delete your browser history you're not deleting your cache and stored cookies, because your computer would still like to keep them because it thinks you might

visit those websites again sometime. When you want to really clean your browser out you'll need to clear the cache and delete all cookies as well.

Downloads and Free computer antivirus software

Hardware? Check. Software? Check. Malware!?

Hardware is the physical computer part, the software is the program you run on the computer so what is malware? Malware is a type of software and the Mal is short for malicious. These are programs that people use maliciously to hurt your computer, spy on you, steal information, or use your computer to attack other computers.

Malware might hide in a song you download or it might disguise itself as a friendly piece of software that seems useful to you. The best way to protect yourself from Malware is know that where you are downloading from is a safe and reliable website and to have a good antivirus software on your computer that also checks for Malware.

Where can I go to download programs safely?

Cnet = download.com

Sourceforge

Varified company websites

Which antivirus software should I use?

PC Magazine (www.pcmag.com) - "The Best Free Antivirus for 2015":
http://www.pcmag.com/article2/0,2817,2388652,00.asp

You are the best antivirus protection for your computer! Really? Yes!