

Introduction to Security Online

When surfing online, it's important to keep in mind some basic principles of safety and security. It may seem like a lot to remember, but soon these tips will seem like common sense when navigating the online world:

- Choose strong passwords and don't share them. A strong password will **not** be a name of someone you know (or your dog), a word, birthday or sequence (12345). Strong passwords combine letters, numbers, symbols, and are over 6 characters.

A good technique for choosing a password is to think of a memorable phrase, then use the first letters of the phrase to create the password.

Memorable Phrase: **my Charlie loves coffee ice cream! at 45**

Password: mClcic!@45

- Don't share personal information unless you are on a trusted, secure site. Check the web address – does it start with **https://** or with **http://**? **https://** is the secure version.



Another thing to check in the website address is spelling. Businesses do *not* misspell their own names in their web addresses – if there is a spelling error, it is a fake site.

- Don't share passwords, bank account numbers, social security numbers, or other sensitive information over e-mail or on a wireless Internet connection that is open to the public. Again, check for the secure site **https://**
- Be aware of scams. Classic scams are: e-mails that appear to come from a friend's account requesting money, notification of prize winnings or other windfalls that require you to send money ahead, and requests for PIN numbers, passwords, or bank account numbers that pretend to come from financial institutions. Just like schemes over the telephone or through the mail, if something seems suspicious online **do not** respond.
- Don't open attachments or go to websites unless you know what they are and that they are from a trusted source. Remember that e-mail accounts do get hacked; if you receive a mysterious e-mail with a website or attachment from a "friend" with no explanation, don't open it!

- Of course, if your friends can have their e-mail account hacked, so can you. If you go to the online help center for your e-mail account provider, you can check what you will need to do if that happens and steps they recommend to prevent it. *Tip – If you don't see a menu with "Help" check for the gear icon that symbolizes "Settings"*
- 
- Don't believe everything you read or see online. . . just like you wouldn't necessarily believe tabloid papers in the supermarket aisle, there are lots of questionable stories on the Internet. Some even come with video. A quick way to check out common pieces of online lore is to enter the claim into **www.snopes.com**
 - Don't forget to fully log out of your accounts. Accounts for e-mail, shopping, banking, bill paying, will all have a "Sign Out" or "Log Out" button near the top of the screen – don't forget to use it, especially on public computers. If you are on a Google account, look for your account name in the upper right corner, click on that once and you will see a box with a sign out button appear.

These tips are some of the basics, which are enough to get started. Check out the following resources to continue learning about being safe online:

Tutorials on Internet basics usually offer sections on Internet safety and security. For example:

- **www.gfclearnfree.org/internetsafety**
(Linked from tutorial site: www.gfclearnfree.org)

For an overview of online security issues check out this government site:

- **onguardonline.gov**

Vermont has an Internet safety program designed for students (k-8th grade), parents and educators called Technicool:

- **<http://www.technicoolvt.org/>**

The FBI warns that seniors are a particular target for scams of all sorts, including Internet fraud. See their page on avoiding common scams here:

- **<http://www.fbi.gov/scams-safety/fraud>**