Email and General Internet Safety Tips

1. Make sure you have anti-virus and firewall enabled. Microsoft Security Essentials is free and recommended. Microsoft Security Essentials was merged into Windows Defender starting in Windows 8, but is a separate download in all other Window versions (XP, Vista, 7).
2. Do not go to any sites that are not trusted. Always verify that the URL in the top address bar matches the domain of where you thought you were going.
3. You need to be able to identify the domain of any URL.
4. Email addresses and hyperlinks contain two portions:
    a. Display Name
    b. Actual Address (Hyperlink address - URL)
5. Never open emails from untrusted sources.
6. Have images disabled in your email program/client.
7. Never click on links in emails, unless you can be certain who the sender is, and that they have sent you something.
8. Never enter trusted information (account info, social security, credit card numbers, passwords), unless:
    a. You absolutely know what domain you are in
    b. That the lock is present on your page (https type address).
    c. You have verified with a known source that the email is legitimate.
9. Understand, most institutions, including banks and major commercial institutions will not ask you for confidential information via email. Always best to go to their site, and see if there are any notifications.

Virus Scanning

You should perform a Quick Scan every few days, and a Full Scan at least once per week.

Definitions

Hyperlink – another name for Internet address displayed in Email or Internet Web page. Clicking on a hyperlink causes your browser to navigate to the new address, sometimes within the same window, and sometimes opens a new window.

URL – Uniform Resource Location, or sometimes referred to as Universal Resource Locator. This is the Internet address – www.harvestchristiancenter.com or http://www.harvestchristiancenter.com.

Domain – Location on the Internet where the website is located, usually designated by a name and extension. The extension can be one of many, but most typically .COM, .NET, .ORG . The domain name is the unique name given and registered to that organization. harvestchristiancenter.com is a registered name. No one else can have this same name on the Internet. However, the name harvestchristiancenter.org belongs to someone else. Notice the change in extension. You should always be able to identify the domain for an address. The domain will always be right before the first slash, or if

there is no slash then it will be the last portion of any hyperlink address. Note, there could be extra names in front of a domain, or following a domain name separated by slash. Look at these examples:

bankofamerica.com – legitimate domain for Bank of America

login.bankofamerica.com – legitimate destination Bank of America

login.bankofamerica.dfw.com – NO. This address goes to the server located at dfw.com NOT Bank of America.

login.bankofamerica.com.dfw.com – NO. Looks legitimate, but also goes to dfw.com.

bankofamerica.com/login.php – good, yes goes to Bank of America server, and to the login.php page on their server.

dfw.com/bankofamerica.php – NO. Goes to a bank of america page on dfw.com website.

Rogue Programs

There are many programs that are masquerading as legitimate virus programs, but are fake. Some of the rogue programs will cause popups which eventually lead you to buy their software to get rid of the problems it has detected on your computer. Some of the names that are out there, and known to be rogue, are:

- Windows Defence Unit
- Windows Prime Defender
- Windows Protection Tool
- Windows Antivirus Suite

Some of these are difficult to remove and may require professional help or additional software.