The Ten Commandments for computers

For Computers

1. Always backup
2. Beware of public WIFI
3. Use unique passwords
4. Always update your computer and programs
5. Use your antivirus

6. Surf smart verify everything
7. Clean up your computer
   a. Remove stuff that you do not use
8. GOOGLE error messages that you get
9. Use nightlight mode
   a. Go to settings
   b. Go to system
   c. Go to display
   d. Turn on night light settings
10. Use the computer club for problems

Commandment 1
Always Backup

<u>Two ways to Backup</u>

1. **Backup with a service**
   - ➢ Back-up services start at $75.00 per year for each computer
2. **Back it up yourself**
   - ➢ Free programs are available to be downloaded
   - ➢ Classes given almost every month at no cost to members

Commandment 2
Beware of Public WIFI

What is public Wi-Fi?

Public Wi-Fi can be found in popular public places like airports, coffee shops, malls, restaurants, and hotels — and it allows you to access the Internet for free. These “hotspots” are so widespread and common that people frequently connect to them without thinking twice. Although it sounds harmless to log on and check your social media account or browse some news articles, everyday activities that require a login — like reading e-mail or checking your bank account — could be risky business on public Wi-Fi.

The problem with public Wi-Fi is that there are a tremendous number of risks that go along with these networks. While business owners may believe they’re providing a valuable service to their customers, chances are the security on these networks is lax or nonexistent.

One of the most common threats on these networks is called a Man-in-the-Middle (MitM) attack. Essentially, a MitM attack is a form of eavesdropping. When a computer makes a connection to the Internet, data is sent from point A (computer) to point B (service/website), and vulnerabilities can allow an attacker to get in between these transmissions and “read” them. So what you thought was private no longer is.

Commandment 3
Use unique Passwords

What Makes a Password Strong?

The key aspects of a strong password are length (the longer the better); a mix of letters (upper and lower case), numbers, and symbols, no ties to your personal information, and no dictionary words. The good news is you don't have to memorize awful strings of random letters numbers and symbols in order to incorporate all of these aspects into your passwords. You simply need a few tricks.

How to Easily Spot a Weak Password

The secret is to make passwords memorable but hard to guess. Learning a few simple skills will make creating strong memorable passwords easy. Creating them can actually be fun - and your payoff in increased safety is huge.

To understand the definition of a strong password, it's best to go over common practices that put millions of users at risk on a daily basis. Let's look at a few examples of weak passwords to understand why these put you at risk:

Check out the CCCGC website at http://cccgc.info/ for a lecture on passwords go t to password presentation

Commandment 4
Always update your computers and programs

Malwarebytes will automatically check for updates

Ccleaner and **Super-Anti-Spyware** have button on them to check for **updates**.

Microsoft Defender

1. Go to settings
2. Go to Update & Security
3. Click Check for updates

Commandment 5
Use and run your antiviruses

CCCGC recommends the following:

Microsoft Defender

Super-anti-spyware (available through Ninite)

Ccleaner (available through the CCCGC website)

Malwarebytes (available through Ninite)

Be sure to update to the lasts version

Commandment 6
Surf Smart - always verify everything

10 Tips for Smart Surfing

1. Be especially careful about using **public or shared computers.** Don’t access personal information on a computer unless you are confident that it, and the network it is connected to, are secure.

2. **Don’t leave your computer unattended** while logged on to online banking or other sites where you provide personal information. Others could gain access to your account information if you walk away.

3. **Always log out** when you are finished to properly end your banking session. That way, no further transactions can be processed until you log on to the system again.

4. **Close your browser** when you finish using it so others cannot view any account information by using the "back" button on your browser.

Commandment 6

10 Tips for Smart Surfing cont.

5. **Practice Safe Surfing & Shopping.** When shopping online, or visiting websites for online banking or other sensitive transactions, always make sure that the site's address starts with "https", instead of just "http", and has a padlock icon in the URL field. This indicates that the website is secure and uses encryption to scramble your data so it can't be intercepted by others.

6. **Disable automatic password-save features** in the browsers and software you use to access the Internet.

7. **Install or update a quality anti-virus program.** As new viruses are created every day, be sure to update your anti-virus program often. Never allow a virus to remain on your computer.

8. **Install or update your anti-spyware program** and scan your computer regularly. Be wary of Internet ads offering downloadable software; in many cases these are fake.

9. **Do not download or install a program** on your computer unless you are confident that it is from a trusted and reputable source.

10. **Keep your operating system up to date.** Computer operating systems are updated periodically to stay in time with technology advances and fix security gaps. Install updates as they come available.

Commandment 7
Clean up your computer

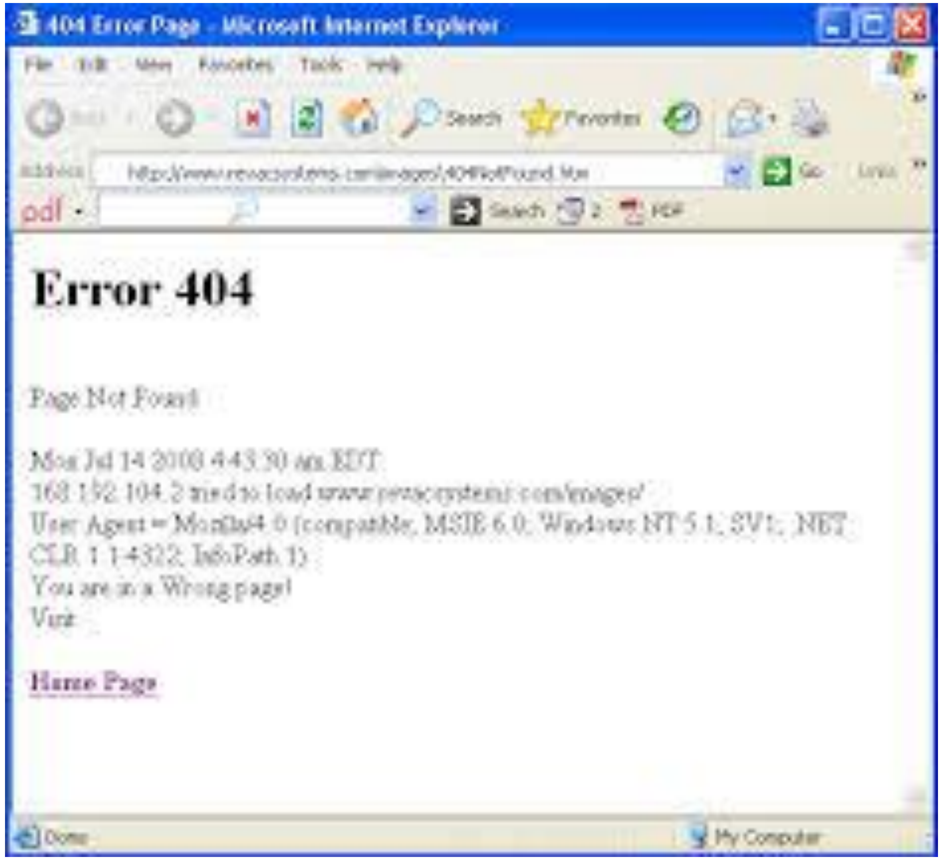
Do your housecleaning on your computer

- Empty your recycle bin
- Check your start-up programs
- Get rid of unused icons on desktop
- Delete old programs you no longer use

Commandment 8
Google error messages that you receive

The **HTTP 404**, **404 Not Found**, and **404** error message is a Hypertext Transfer Protocol (HTTP) standard response code, in computer network communications, to indicate that the client was able to communicate with a given server, but the server could not find what was requested.

The website hosting server will typically generate a "404 Not Found" web page when a user attempts to follow a broken or dead link; hence the 404 error is one of the most recognizable errors encountered on the World Wide Web.


404 Error Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
http://www.revacsystems.com/images/404NotFound.htm
Go
Links
Search
PDF
Done
My Computer

Error 404

Page Not Found

Mon Jul 14 2008 4:43:30 am EDT
168.192.104.2 tried to load www.revacsystems.com/images/
User Agent = Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; InfoPath.1)
You are in a Wrong page!
Visit

Home Page

Commandment 9
Use the new nightlight mode

- ➢ Go to settings
- ➢ Go to systems
- ➢ Go to display
- ➢ Turn on the night light settings

Commandment 10
Use the computer club for help or problems

Charlotte County Computer Group Corporation
2280 Aaron Street
Port Charlotte, FL 33952

Phone: 941-585-0356
941-625-4175 x244
E-mail: office@cccgc.net
Website: www.cccgc.info

Office Open: Monday – Friday, 10:00 a.m. – 2:00 p.m.

The Ten Commandments for computers

Microsoft will never call you