

COMPU 360 BYTES

VOLUME 8 - 2011

AUGUST, 2011

This FREE newsletter offers news and tips to our customers regarding upcoming trends in technology.

Our goal is to keep our customers well informed about computer technology.

IN THIS ISSUE:

Your Computer - How to keep it secure 1

History Sniffing on the Internet 2

Windows 8 Already! 2

Microsoft Office - Using Templates 3

Compu 360 News 4

Your Computer — How To Keep it Secure

It is very important to keep your computer secure. Intruders want your information, like credit card numbers, bank account number, e-mail account information, and so on. By stealing information, intruders can use your information to purchase things for themselves.

Another way that intruders use your computer is by installing malicious software (Trojans, worms, and so on) to get your information or use your computer to send out Spam e-mails.

There are some steps that you can take to ensure that your computer is secure.

1. Install Anti-virus software – Such software scans every file on your computer for known pattern and match it to virus signature. Then, the anti-virus software offers various ways to remove or handle such malicious files. Unfortunately, there are thousands of computer viruses created every day. If you use the Internet, read e-mails or download attachments, and so on, you need a good anti-virus software.



2. Install a Firewall – There are two different kind of firewalls: software firewall (usually offered by software manufacturers which sell anti-virus software) and hardware firewall (comes with your router). It is best to have both types of firewalls for your computer.

3. Careful when reading your Emails – Emails are very convenient and used widely to communicate. We all receive e-mails with attachments. Be careful downloading/opening these attachments. Also, be careful about e-mails which ask you to

click on a website link. DO NOT provide any personal information based upon a link that is provided to you in an e-mail. Banks, credit card companies, or any vendors which you use to make online purchases, do not e-mail you asking your passwords or login information Be careful of such Phishing tricks which ask you to provide your personal information.

4. Use Strong Passwords – It is a good idea to have a password to login to your computer. You also need to ensure that your password is strong, both to login to your computer and for your email. It is never a good idea to type your password in a document and saving it on your computer. A strong password may contain special characters like “@” or “!” sign. It may contain six or more characters (letters and numbers). However, make sure that you REMEMBER your password, otherwise you may lock yourself out of your own system or e-mail account.

5. Keep your system updated – If you are using a personal computer (PC), Microsoft (and also Apple), and other vendors like Adobe, release software upgrades whenever they discover that there is a weakness in their software. These “patches” close the security loopholes in their software. Make sure that you update your system.

6. Use File Encryption – File encryption programs help you encrypt files so that they cannot be read unless correct password is provided to open them.

History Sniffing on the Internet

Imagine that you are on your computer browsing the Internet and some dubious program is tracking the websites you visit.

When you visit a website, your browser remembers it. So, the next time you look for that site on a search engine, it shows up in a different color (usually purple). This way you know that you have visited that site previously. Unfortunately, this also means that a spyware can look into this history.

Earlier versions of the Internet browsers did not prevent against malicious software from looking into your Internet browsing history and collecting information regarding your Internet browsing habits. However,



er, the later versions of Internet Explorer and Firefox have tried to stop this. Apple's Safari and Google's Chrome Internet browsers were first to address this issue.

To ensure that you are not a victim to history sniffing, make sure that you upgrade your browser to the latest version available to ensure that you have the latest version available which will offer the latest security features.

Most of these attacks come when you use an Internet browser (Internet Explorer, Firefox, Chrome, Safari, and so on). So, first make sure that you have the latest browser installed on your computer.

Next, make sure that you have tightened the security aspects of your browser to prevent any kind of history sniffing.

It will also help you to learn safe Internet browsing techniques so that you are safe while browsing the Internet.

Windows 8 Already!

Just when we were getting used to Windows 7, Microsoft announced in June 2011 their new operating system (OS) — Windows 8.

The demo of Windows 8 showed some ways the new OS will work with the new generation of touch centric hardware. It will also come with fully touch-optimized browsing for Internet Explorer 10 (IE10). In IE 10, we will be able to switch among tabs just by using our finger (assuming you have a touch screen).

Windows 8 will tap into the power of HTML 5 (Hypertext Markup Language 5), using standard Javascript and HTML to



deliver apps which will be touch-optimized.

In the demo, the Start screen is personal mosaic of tiles. Each app will be represented by a tile. So, for example, weather app will appear as a tile which will give you the weather information without clicking on it.

Switching among applications appears to be seamless. If you have touch screen, you can simply move between applications by pointing and moving a finger.

A feature called "Snap" will allow you to snap apps next to each other, and then switch between apps easily.

It will also allow easier access to files, like pictures from different apps on your computer or from other computers which are sharing files with your computer.

But, Windows 8 is only in beta testing phase and a lot will change between what we previewed versus the final product.

Microsoft Office - Using Templates

In this article, I am going to discuss how to use templates to create Word documents. However, the same technique can be used for other Microsoft Office programs (Excel, PowerPoint, Publisher, and so on).

Templates are pre-formatted documents (or worksheets in Excel, slides in PowerPoint, and so on). Each template is designed with different attributes and can be used for different purpose for example, agendas, brochures, business cards, calendars, and so on.

Each template includes placeholders with instructions on what to type in certain placeholders.

To access templates in MS Word 2010, click on the **File** tab, then click on the **New** option.

You will notice the various templates in the right-hand pane of this screen.

You can choose the template type that best fits

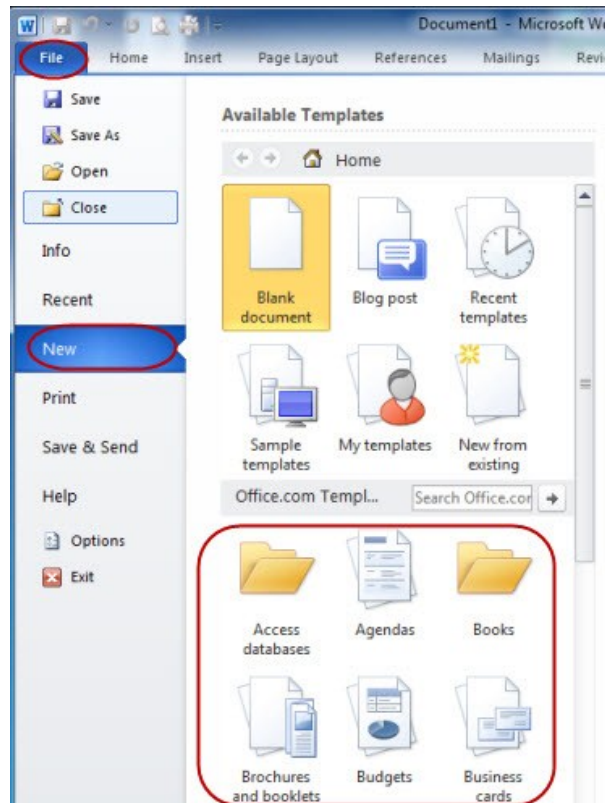


your needs. In this article, I am going to choose "Newsletter" template.

You will see various newsletter templates.

Browse through the templates and pick one that closely matches to your needs.

Click the **Download** button from the right-pane. You will notice that the template that you choose will be downloaded on to your computer. Once



the template is downloaded, it will open as a document in MS Word.

Now, you can select text that you want to delete and type your own text in the newsletter. You can also change images, font type, color, size, and so on.

Customizing a Template

A templates provides you a starting point. You can change images or text box holders in the template to change the look and feel of a template.

Create a Template with Hidden Tab

You can also create a template out of a document that you regularly use. To do so, first you will need to the downward pointing arrow and then



click **More commands**. From the Word Options window, click on Customize Ribbon and then click in the **Developer** check box.

You can click placeholders which you want to be editable and areas which you want to restrict making changes.

After making all changes, choose File, then choose Save As option to save this document as a Template (by choosing file Save as type as Word Template) and save it in My Templates.



In Our Store or At Your Door

**4877 Dover Center Road
North Olmsted, OH 44070**

Phone: 440-779-0360

E-mail: info@compu360.com

Quality Computer Solutions for Home or business. We can save you up to 50% or more as compared to other computer repair or web design service.

Compu 360 specializes in computer repairs, virus removal and anti-virus installation, software upgrades, web design, and database programming. We provide a variety of services thus saving you money, time and the hassle of shopping around for different vendors for quality and professional service.

We offer all of our services for individuals or businesses.

Coupon!!!

Call us for Service & mention the code: PC360 to save \$20 Off Any Service

Seniors save an additional 5% on Any Service.

Save up to 50%

Compu 360 News



We recently opened our first store in North Olmsted .

This enables us to serve you at our location or on-site.

Please call or e-mail your comments or suggestions to us and let us know how we can serve

For a full listing of the services that we provide, please visit our website at:
<http://www.compu360.com>

