TECH NEWS THAT YOU CAN USE

October 2016

26056 CENTER RIDGE ROAD, WESTLAKE, OH 44145 **TEL: 440.871.9300**

We, at Compu 360, believe that our customers are a part of our family. Our role in your technology world begins with a simple call or visit to our store. However, that is just the beginning of our relationship. Through this newsletter, we intend to keep you up-to-date with the latest technology trends and other useful technology information that you can use in your daily life. Please visit our site at http://www.compu360.com and let us know as to how we can improve our services and offerings to better meet your technology needs. *Arun Singh*

Password Managers

In our experience, a lot of people use weak password because they find it difficult to remember complex passwords. For example, many people we know use passwords which have the name of a person and certain date which has some meaning in their life, like a birthday, anniversary, and so on. Trying to remember dozens of complex passwords is difficult, if not impossible. Password managers seem to resolve this problem. In this article, I would like to discuss how to use password managers and get the most out of them.

Different passwords for different accounts

We hear about password leaks or hacking often, with the latest major one at Yahoo where over 500 million Yahoo accounts were breached. If you have different passwords for each online account, it helps you to only have one of your account passwords getting compromised, while others are not affected. Password mangers help you by saving all your online account password and encrypting them.

Complex passwords

Most of the password manager software are capable of generating complex passwords for your online accounts. Websites encrypt your passwords, but depending upon algorithm used these passwords can be cracked. The more complex a password, the less chance that an attacker will be able to crack it. Currently, a password with 12 or more characters is a good number to look for. You should use upper and lower case letters, numbers, and special symbols allowed by a particular website.

In order to use a password manager, you will need to remember a master password. This will allow you to login to your password manager. It is also a good practice to remember the password to some of your critical accounts, like e-mail. This way, if you forget the password to the password manager, you can reset it using your email account information. So, what would be an example of a complex password? A phrase that you can easily remember but would be hard to guess, for example, 3Hamsters2Mice1GuineaPig! Such passwords are phrases and easy to remember even though they are longer than 12 characters.

Offline vs. online password managers

Some password managers are offline, like Password Safe, Enpass or KeePass. Offline password managers do not synchronize information across all devices. Others are online password managers, like LastPass, DashLane, 1Password, automatically synchronize passwords across different devices. Some provide web-based access to your password vault.

Master password can be cracked, so don't rely on it alone

So, here is a scenario: you have stored all your password in a password "vault" and then protected the password vault with a master password. What if someone hacks into your master password? If that happens, then the attacker will have access to all your passwords. This is a bad scenario. Many password managers offer two-factor password authentication. In this case, access to your password vault requires a password and a one-time code that is sent to you via SMS to your phone by the password manager. So, if someone gets your master password, your vault is still protected. If you get a SMS with a code and you have not tried to access your password vault, then this should server you as a notice that your master password may be compromised. If so, please change your master password IMMEDIATELY.

Use Password Manager's security features

These days, we use multiple devices and a lot of times we forget to log out of our accounts, like e-mail, bank, and so on. Some of the password managers offer the option to log you out automatically if you have been inactive for a certain amount of time. This helps if someone logs into your account by just pressing the "Back" button on the Internet browser.

Another helpful suggestion is NOT to flag a device as "trusted", as this disables two-factor authentication on that device.

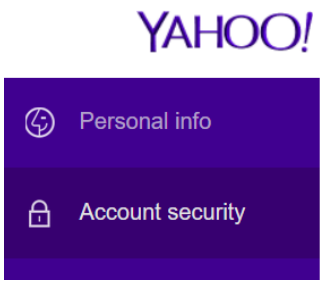
So Your Yahoo data has been hacked, how do you change your Yahoo password

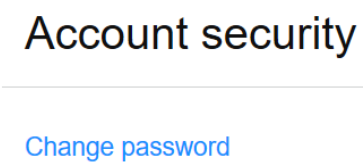
Yahoo announced that more than 500 million Yahoo users' accounts may have been breached and their information stole in late 2014 (and we are just finding about this last month in 2016!). Well, I have noticed that some of our customers' Yahoo passwords have been stolen and their e-mail accounts have been used to send malicious links in e-mails to me. As soon as I noticed this, I notified those clients to change their passwords immediately.

This breach of information is pretty big and will affect over 500 million users. I recommend that you DO NOT wait to see if you are one of the Yahoo users whose information has been stolen. Please changes you Yahoo account password IMMEDIATELY.

To changes your Yahoo account password on a computer:

1. Log in to your Yahoo account using your current information.
2. Take your mouse pointer to your username and from the drop-down menu, click on "Account Info"





3. From the menu on left, select “Account Security”
4. Click “Change password”
5. Follow the tips in the first article of this newsletter to create a strong password and change your password.
6. Click “Continue”

To change your Yahoo account password on a mobile device:

1. Log in to our Yahoo account
2. Tap the Menu button
3. Click on “Options” (this icon looks like a wheel)
4. Under “Account Security”, click “Change password”.
5. Create a new password, confirm by re-typing the same password.
6. Save the new password.

Note, it is a good idea to enter your cell phone number in your account information. This helps you in case you forget your password. Yahoo uses your cell phone number to send you a one-time code to your SMS. This can be used to authenticate you as the owner of your Yahoo account.

Cyber attacks and your device security

Most of the devices which can be connected to online access of some kind are susceptible to attacks. Follow the following tips to enhance the security of your devices to make them less susceptible to attacks:

- Make sure that you know which of your devices are Internet-accessible. For example, Smart TVs, DVRs, smart phones, computers, tablets, and some new refrigerators, to name a few.

- If you purchase such a device, read some reviews about that product and brand name to get an idea about its security features and their review by other customers who have used that product.

- Stay away from counterfeit products as they may have security weakness, or even worse, have malware intentionally embedded in the software of that device.

- Use the “embedded security” and its features that come with the device.

- Keep the software of such devices up-to-date with all the security updates. Manufacturers of these devices are constantly researching security loopholes and releasing security updates, once they find such loopholes.

- Your home Wi-Fi is awesome to use, but you MUST secure your home network. Remember to use the password tips discussed in this newsletter to come up with a complex password. Also, for your router, following recommendations come-in handy:
    - Change your router name and your network name from generic names, like Linksys0242, Netgear245, etc. to different network names. This prevents attackers from guessing which brand Wi-Fi router you are using.

- You can hide broadcasting your network name. This reduces the chance of someone even knowing what your network name is. A person will only see the term “Hidden Network” when one tries to connect to it. In such a case one needs to know the network name, otherwise one cannot connect to your network.

- Setup a different network password for your home network and a separate password for your guests. This prevents your guest/s from accessing your personal network resources.

- Change the network IP address that is provided by your router manufacturer (the general ones are: 192.168.0.1, 192.168.1.1, 192.168.1.0, etc.) Changing the IP address to something like 1.1.1.1 adds to the complexity and makes your network more secure.

Note: Some of the items discussed in the list above are NOT basic networking issues and may need to be addressed by an IT professional. If you are not sure as to how to make these changes, please call us and we will be more than glad to address your network security concerns.

Tech Support Scam!

According to Microsoft’s Digital Crime Unit, about 3 million people fall victim to tech support scam every year. Are you one of them? Have you received a call from someone claiming that he/she is from Microsoft (or Windows) tech support and that your computer is sending error messages? Or have you called a tech support thinking that you have called Norton, McAfee, Apple or another such company, when in fact, you have called a tech support scam?

These scammers ask you to give them remote access to your computer via the Internet and they will show you the problem with your computer and fix the problem. Once you give these scammers access to your computer, they digitally crawl your computer and steal your digital information like your password, account numbers, and any such information that you have stored on your computer.

As if that is not bad enough, these scammers then may leave some malware on your PC that allows them access to your computer at any time and use your computer to send out spam e-mails to other people.

Another clever way that these scammers may try to reach you is by opening up a website window on your computer which gives you a warning message with a phone number to call. In certain cases, such a screen or pop-up window will not let you close out your browser. Also, this window may come back if you shut down and restart your Internet browser.

We have seen numerous such computers which have been infected by such scammers. Some computer users have also used their credit cards and paid these scammers around $400 or more only to find out that their computer stay infected after these scammers ‘clean’ their computer and remove the malware.

So, what should you do if you or someone you know has been a victim of such a scam?

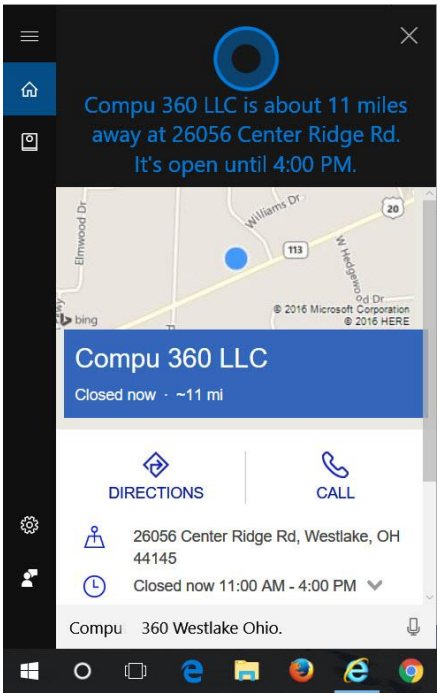
- Please DO NOT allow anyone to remotely access your computer, unless you know the person or company who is asking you to remotely access your computer.

- Freeze your credit card by contacting your bank or Credit Card Company.

- File a complaint with the Federal Trade Commission (FTC) by going to this website: https://www.ftccomplaintassistant.gov/

- Contact us immediately so that we can discuss with you the course of action that you should follow to rid of the malware or any issues with your computer. We will also guide you as much as possible for the course of action you should follow in future so that you do not fall prey to these scammers.

Windows 10 Assistant – Cortana



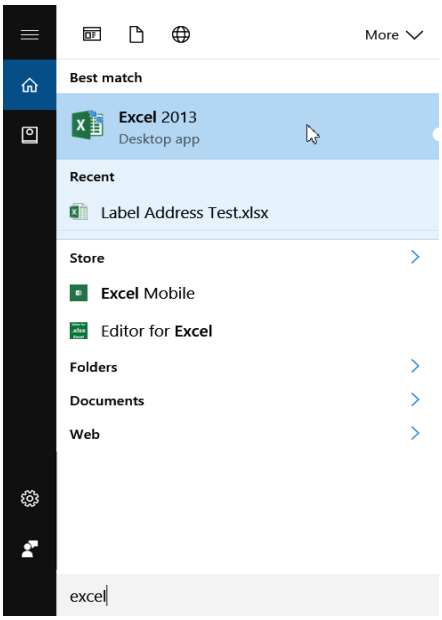
Windows 10 has provided you with a personal assistant "Cortana". It can monitor your online activity and also provide you helpful reminders. Cortana interacts with Microsoft's "Bing" search engine to provide you with results that you seek.

The same functionality is also available on Windows phones and devices that you use by signing into your Windows account. Please note that Cortana will ask you to allow it to use your current location to provide you with search results. If you so choose, you can deny location tracking information and just type in the search query in its search box.

Cortana can be activated from the sidebar using the voice command "Hey, Cortana".

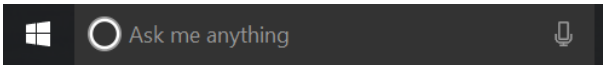
To initially setup Cortana, click on the search box and provide the information that it requires. However, if do not wish to setup Cortana, then you can simply click and type your search keyword or phrase in the search box and Windows will provide you with the search results.

Search your computer and the web



In the search box (next to the Start button), you can type in your search keyword or phrase. If Windows finds an app, folder or file related to your search, it will display the results, along with other options on the web where you can either purchase an app or a website where you can find additional information regarding your search.

Has it happened to you that you may know a file name or something about a file that you have created in the past and now forgotten as to where you saved it? Well, the search box in the taskbar is the place where you can type in your file name or a



keyword. Windows will look in your folders on the computer and will try to find all

files which have that keyword in their name or even somewhere within a file.
