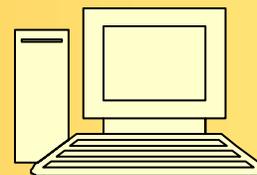


BAY BYTES

Greater Tampa Bay Personal Computer User Group, Inc.



Newsletter

Issue 10

October 2012

26th Year of People Helping People!



In this Issue

What is the Cloud, anyway	2.	2
Insert text on to digital pictures		3
Digital estate planning tools		4
Un-send e-Mail letters		5
Un-send e-Mail letters	2.	6
Un-send e-Mail letters	3.	7
What is Malwarebytes		8
What is Malwarebytes	2.	9
The lighter side		10

Don't forget to visit our club's site at:

<http://gtbpcug.org>

As well Don Miller's and Darrell Manns' :

<http://www.dmanns.org/dmiller/>

What is the Cloud, Anyway?

By Rich Maloof



Photo: Pascal Preti/Getty Images

There's a lot of buzz lately about "the cloud" but not a great deal of understanding among the people, like you, who are going to be using it. Here's a quick primer — with minimal tech talk — to explain what cloud computing is all about.

If you're feeling a little knuckleheaded for not having grasped the concept of cloud computing, by the way, you're not alone. In a recent survey only 16 percent respondents knew what the cloud was even though 95 percent using it at home and at work. We're in the midst of a massive transition to cloud computing, and with a little understanding we can get a lot more out of the technology.

"Once people are moved into the cloud, they recognize they can improve on productivity, costs, security, and efficiency without changing the way they do business day to day," explains Mike Quick, Client Relationship Manager for Cloud Strategies, a Microsoft partner that specializes in migrating organizations onto cloud networks. "All of their productivity is shifted online, accessible 24/7 from anywhere in the world."

Continued on the next page

What It Isn't

First things first: There's no real cloud. A cloud is actually a server, which is a centralized computer (or network of computers) with enormous storage capacity locked away in a windowless building somewhere. Thanks to superfast Internet connections, our own computers and devices can access those distant servers without perceptible delay. The upshot is that we can capitalize on the massive storage and function of cloud servers just as easily as we use the memory and hard drives resident in our laptops, desktops, smartphones and tablets. So, it doesn't matter whether the files and programs you're using are on the cloud or on your own computer: the user's experience is virtually transparent.

You're on It

If you use Web-based email such as Hotmail or Gmail, you're already on a cloud. The software application that runs each of those email programs is on a server at Microsoft or Google, and so are all of your messages. You control the program through your computer, but the processing and storing of your email is happening on a cloud.

Think of it like keeping money in the bank. You don't need your money to be in your pocket. You control it remotely, using your credit cards and checks to tell the bank what to do with it. Without ever having cash physically in your possession, your money is out there to use as you please. In cloud computing, the cash is your files. The bank is the cloud. You don't need files and applications to be stored on your computer to use them. They're out there on the cloud and you control them remotely from your desktop, manipulating and sharing them any way you please.

Hey, You — Get onto My Cloud

Web-based email and offerings such as Google Docs are a typical user's first steps toward cloud computing. Because cloud servers can run all kinds of different applications and store files of any type or size, the possibilities run sky-high. A cloud can run Excel and store all of your spreadsheets; run PowerPoint and save all of your presentations; and run QuickTime and save all of your home movies. You can store or "push" all of your photos, music, and contacts to the cloud.

Here's where cloud computing really starts to pay off: Whatever you store on a cloud can be accessed from anywhere. And because anyone with permission can access the data, there's enormous potential for collaboration. Imagine three people in neighboring towns, looking up at the sky. They can't see one another other but they can all see the same cloud (that is, a real cloud of the cottony white variety). Online collaborators can "see" the same cloud server and make changes to shared documents, as many businesses and families already do with online calendars. There's no emailing of cumbersome files or keeping track of a latest version — the file sits in one place where all collaborators can view, edit and save it.

In the same way, the files you store on a cloud can be accessed by any of your own devices. If you've stored a song on a cloud, you can access it from your laptop, your Smartphone or your desktop computer. Travelers can push vacation photos to the cloud before leaving for home, and business road warriors never have to worry about losing a customer presentation. It's as if all your stuff is floating above you, available to be pulled down whenever and wherever you want.

Current Examples:

Plenty of cloud-based offerings are already being heavily marketed and used by consumers, from Spotify's streaming music to Apple's iCloud to Amazon's Cloud Reader for the Kindle. Users find value in them for storage and backup, though they're a different breed from the broader and more customizable services such as Google Drive, where you can store, search, edit and collaborate using different Google programs and a variety of file types. Personalized systems for consumers are taking a page from the sophisticated cloud technology being adopted by businesses. Like consumers, corporations have been a bit slow to understand and adopt, but the potential benefits are sending more people into the cloud every day.

From the Computer Lady

<http://www.computerlady.org>

Dear Computer Lady,

Q: When I pick a picture from "My pictures" (It may be a picture from an E-mail, Newsletter or magazine that I have saved as) to E-mail to a friend; I would like to put a comment under the picture.

It doesn't work for me as it won't let me type on the picture copy page.

Can you advise me if this is possible or perhaps I should "save picture as" differently???

A: What you need to add text to a picture is an image editing program. There are many image editing programs out there, but if you are using a computer with Windows on it you already have a basic image editing program included called, Paint. You can easily open your image in Paint, add text, and then save a copy of the image with the text added. Here is how:

1. Open Paint by clicking Start, pointing to "All Programs" then "Accessories" and finally click on "Paint".

An alternate way to open Paint in Windows 7 is to click on "Start" and then type "Paint" in the search box.

2. Once you have Paint open, you can open your image using the file menu (Or click on the tab on the very left).

3. With your image open, you can then use Paint to add text to your image.

Another tool that you can use to put text on an image is Picasa at:

<http://picasa.google.com/>

Picasa is a free image program from the folks at Google. When you open a picture in Picasa, just click on the wrench in the upper left corner of your screen, then click on the text editing tool (It has ABC on the little icon) and add your text.



Sample picture submitted by
a GTBPCUG member

Do You Have a Digital Estate Plan?

<http://www.askbobrankin.com>

What will happen to your email, Facebook, iTunes and Amazon accounts if you die? It's an uncomfortable question, but leaving it unanswered can be vastly more distressing and costly for your loved ones who survive you. Here are some tips on setting up a digital estate plan...

You Can't Take Them With You...

Recently, there was a rumor that actor Bruce Willis was planning to sue Apple for the right to leave his iTunes music collection to his children. There was also a story about Steve Jobs being reincarnated in a parallel world. The Willis rumor was debunked, and I'm pretty sure that Steve won't be checking his email any time soon.

Sooner or later, we'll all kick the bucket, buy the farm, or shed the mortal coil. But when you go, what will happen to your online accounts? You may or may not be content to just leave your Gmail or Facebook account dormant. You may have photos or documents in cloud storage. What if you have money in your PayPal account? And will your surviving relatives have the keys to your online banking or investment portfolio?

Also keep in mind that email and social network accounts can get hacked. Families and friends have been traumatized by spam sent from the accounts of the deceased. It can be difficult for survivors to get online accounts shut down after someone dies. Sometimes, it requires an expensive lawsuit or other court action.

Facebook, Twitter, Gmail, and some other major [online services](#) have procedures for handling the accounts of deceased members. In most cases, they require faxed copies of a death certificate, the photo ID of the requestor, and a notarized statement of authority. But Amazon, [Grooveshark](#), Foursquare, and many others don't publish any information about dealing with deceased members' accounts. The [DeceasedAccount](#) website offers a handy guide to the deceased-member policies of many online services. The simplest solution is to write down all of your accounts and their login credentials, then give that list to someone you trust. Of course, you'll have to remember to constantly update that document when you [change passwords](#) or create new accounts. But what if you don't trust anyone with all of your digital keys, at least while you're still alive?

Digital Estate Planning Tools

[DeadmansSwitch.net](#) lets you send emails after you die. An email to your executor, for instance, might contain a list of accounts and passwords or a full-blown digital will and testament. The service sends a check-in email to you every so often; you confirm that you're still alive by clicking on a reply link. If you don't reply within 60 days, you are presumed to be dead and your stored emails are sent. The free version supports up to two recipients. For a one-time fee of \$20, you get up to 100 recipients and the ability to customize the check-in intervals and reply deadline.

[SecureSafe.com](#) adds cloud storage to the posthumous email solution. You can [upload documents](#) and other files that will be sent to recipients upon your presumed death. Each file gets assigned to a beneficiary, so you can leave different things to different people. The free version supports storage of up to 50 [account passwords](#), while paid versions provide more storage space and security such as two-factor authentication that beneficiaries must provide to access their bequests.

[The Digital Beyond](#) is a news and information site devoted to digital [estate planning](#). It offers a directory of services similar to those mentioned above; links to news articles on the subject; and a book called, "Your Digital Afterlife" that can help you consider what your digital legacy should be and set it up according to your final wishes. What do you want done with your email after you die? Many people want a relative to login and send a message to all contacts with their news of their passing.

Should your Facebook page be closed or converted into a "memorial page"? How much money do you keep in PayPal, and who should get it when you die? How about your digital photos stored on Flickr? Do you have a blog or website that may need to be closed down? These and many other questions are worth answering before you go.

Can I stop or 'un-send' an email I sent by mistake?

<http://ask-leo.com/>

Once you hit that Send button, you must assume that there is simply no way to stop your email from being sent ... even if it's to the wrong person.

Q: I wrote an email from my Yahoo email account and sent to the wrong email address in Europe. Is it any way that I can retrieve the email I sent from the wrong email address and delete it before the wrong recipient can read my email?

A: No.

There are a couple of exceptions – one of which isn't really an exception at all, but the answer you need to keep in mind and always remember is simply **no**.

Once email has been sent, it has been sent. I'll describe why that is and what those so-called "exceptions" are all about.

When you hit Send...

When you hit the **Send** button, the following happens:

"Once an email leaves your outbox, you lose all control over it."

If you're using a PC-based email program, like Outlook or Thunderbird, the email is sent from your machine to your email provider.

The email is then sent from your email provider to the email provider of your recipient.

The email is then placed in the recipient's online inbox¹.

If the recipient is using a PC-based email program, he downloads it to his machine. Two things are important to realize about that scenario:

The first three steps – up to and including your recipients' online inbox – can often happen in seconds².

Regardless of which steps have and have not occurred, it's all out of your control once the sequence begins.

Once an email leaves your outbox, you lose all control over it. And I do mean *all* control over it. You cannot stop it. You cannot change it. You cannot track whether it's been read or not. You cannot tell if it's been forwarded or deleted. You can't even know whether it's been received at all unless you get some kind of response from the recipient.

Not really an exception: Gmail

Many people point to a feature in [Gmail](#) and tell me, "But, but ... Gmail lets you unsend!".

Continued on the next page



No. No, it does not!

Read the description of that feature (available in the "Labs" section of Gmail options). All that this feature does is *delay* the send for a few seconds. In other words, when you hit the **Send** button, *Gmail doesn't send the mail.*

At least, not right away.

After a few seconds, it does. And once it does send, then the Undo feature is no longer available for that message, because once email is actually sent, it cannot be un-sent.

All this feature does is give you a few seconds to change your mind. During that few seconds, the mail has not yet been sent.

An actual exception: Some corporate systems

"Corporate" here is really just a characterization because of course, these email systems could be used elsewhere. It's just more common to see them in large corporations.

Some of these email systems have a real, honest-to-goodness un-send option.

However, there are a couple of requirements:

- The sender and the recipient must both be on *the same mail system*. I'm *not* talking about Gmail or Hotmail or whatever, here. I mean that both sender and recipient likely work for the same company and use the same email system *as provided by that company*.
- The email has not yet been read by the recipient.

It's possible that an un-send function will actually remove your message from the inbox of the recipients.

The last item is hopefully obvious, but if they've read the message there's no way to make them un-read it. Once seen, it cannot be unseen. You might be able to "remove the evidence" in that perhaps the message might have disappeared from their inbox, but even then, they could have copied or printed it before that happened.

And again, this is not, **not, NOT** available with the email services available on the internet and not something that would work between differing email services even if it was.

Continued on the next page

An embarrassing exception: Recall

Some email programs and some email system expose a function called message recall.

The intent was – like Return Receipt – to provide a semi-standard way to "recall" or bring back a message that had been sent. In other words, a way to un-send it.

And much like Return Receipt, it's not implemented or it simply doesn't work as intended in most email programs.

When I've seen this attempted, the cure seems much worse than the disease.

The problem is simple: when recall is used, it works by sending another email message to all the recipients of the original message that says:

[Sender] would like to recall the message [Subject]

Now, I'm sure that the idea is that the message would never be seen by the recipients and that the mail programs would just recognize some special headers and perform the recall function by deleting the original message from the recipients inbox.

In practice, that's not what happens.

What usually happens instead is that everyone who got your first message by mistake now gets this second message drawing even more attention to the mistake.

I'm sure it works on some systems somewhere, but make darned sure you understand whether or not it won't just make people take special attention to your original mistake. Much like a politician attempting to delete evidence from the internet, there's a very good chance that all it really will do is make people take even more notice of whatever it is you're attempting to hide.

The moral of our story

There is no undo send. Even if there were, you still run the risk of people reading the email before you hit Undo. Once email is sent, you lose all control over it; *all control*.

Bottom line: make sure you *really* mean it when you hit **Send**.

1: We normally think of web-based email services like Hotmail or Gmail having online or web-based inboxes. In reality, almost all email services provide web-based [interfaces](#), even if they are never used. Email can appear in these web-based inboxes almost immediately.

2: Even though the entire infrastructure of email is designed to tolerate delays measured in days, and we occasionally see that, more often than not, email is currently delivered in a matter of seconds.

Is Your Internet Security up to Date?

Antivirus up to date?

Firewall?

Windows up to date?

Spy Ware?

See how to protect your computer at:

<http://gtbpcug.org/protect/>



More about Internet Threats

What is Malwarebytes... It's not an anti-virus tool

<http://www.askleo.com>

The folks in the Malwarebytes forums are quick to point out that Malwarebytes Anti-malware isn't a substitute for anti-virus software. In fact, if you run Malwarebytes Anti-malware, you'll see that they explicitly recommend that you run anti-virus tools in addition.

I run (and recommend) Microsoft Security Essentials as my anti-virus tool.

"What Malwarebytes Anti-malware has a great reputation for is simply this: removing malware that other tools miss."

It's not quite an anti-spyware tool

Another characterization that you'll not find anyone using is calling Malwarebytes Anti-malware an anti-spyware tool.

While that's perhaps the closest or least inaccurate characterization, I've noted that the folks at Malwarebytes avoid calling it that. In a sense, the term is too vague anyway; to the extent that most people think of "spyware," it's also perhaps too limiting.

So, I also run (and recommend) the same Microsoft Security Essentials as my anti-spyware tool.

So just what is Malwarebytes Anti-malware?

As it turns out, Malwarebytes is hard to pigeon-hole. It has characteristics of both anti-virus and anti-spyware tools and it certainly removes things that we might consider viruses and spyware, and yet it's not really a complete solution for virus protection, although perhaps it's close to a solution for anti-spyware. And yet - those terms just don't cover or characterize the tool properly.

Hence, it's an anti-*malware* tool.

Continued on the next page

Why I recommend it

What Malwarebytes Anti-malware has a great reputation for is simply this: removing malware that other tools miss.

The nature of the race against malware means that no single anti-virus or anti-spyware tool is going to detect and remove every possible infection. No tool is perfect.

When faced with someone who suspects or has all the indications of their machine being infected with malware of some sort, my instructions almost always boil down to this:

- Run an up-to-date anti-virus scan, making sure that both the anti-virus tool and its database are as up-to-date as possible.
- Run an up-to-date anti-spyware scan, making sure that both the anti-spyware tool and its database are as up-to-date as possible.
- Consider running a scan using the free Malwarebytes Anti-malware tool.

That last line is there simply because experience shows that even up-to-date scans with good anti-virus and anti-spyware tools can still miss things, things that Malwarebytes Anti-malware will sometimes catch.

Running Malwarebytes Anti-malware all the time

Like many anti-spyware and anti-virus products, the PRO version of Malwarebytes Anti-malware can be installed and instructed to run regularly scheduled scans.

There's absolutely nothing at all wrong with that. Used *in addition to* a good anti-virus program, it provides an added layer of security. Even though it overlaps in some ways with anti-spyware tools, running it in addition to one of those may also be a reasonable solution. It's possible (although I have not confirmed) that it's not unreasonable for MalwareBytes Anti-malware to take the place of an anti-spyware tool.

That's just not how I use it, and it's not the scenario that I end up recommending. Nothing against that scenario; it's just not the way I use Malwarebytes.

Why Malwarebytes Anti-malware isn't installed on my machine

Put a different way, I consider Malwarebytes Anti-malware a great *on-demand* solution, and I run it only when I feel I need to. If I suspect that there is malware of some sort on my machine, then I absolutely grab the latest version of Malwarebytes Anti-malware and scan the heck out of my machine.

I just don't bother installing it until I run into that situation. Fortunately for me, that doesn't happen very often. Unfortunately for others, however, it does, and as a result, Malwarebytes Anti-malware is something I mention to people almost daily.

Malwarebytes Anti-malware, I recommend it!

Leo

Show the menu bar in Windows 7 Explorer

<http://windows.microsoft.com/en-US/windows/home>

The classic menus from Windows XP are still available in Windows 7, but they're hidden by default. You can show them if you need to, although most of the same tasks are available on the toolbar or on the menu that appears when you right-click a file or folder.

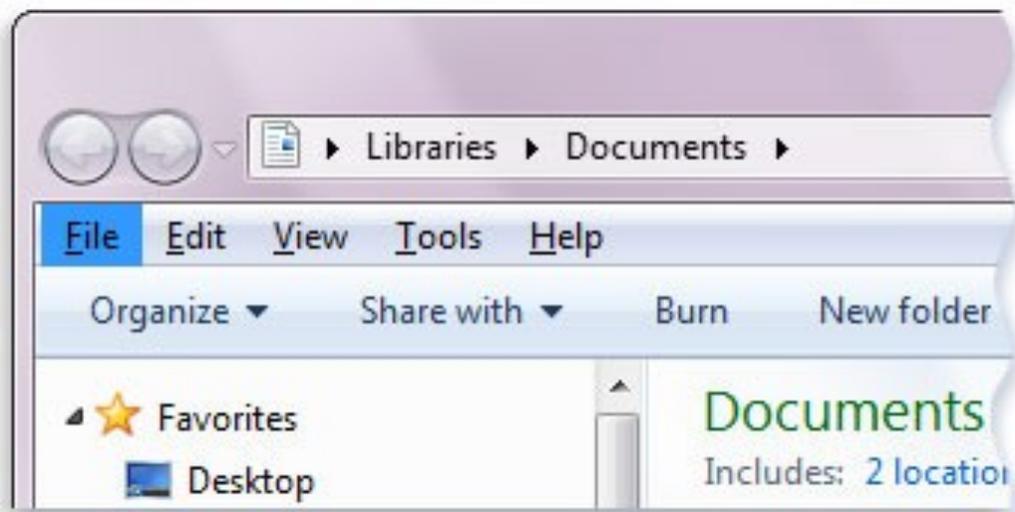
To show the menu bar temporarily

1. On the taskbar, click the **Windows Explorer** button.
2. Press the Alt key. The menu bar appears above the toolbar
3. To hide the menu bar, click any menu item or press Alt again

To show the menu bar permanently

1. On the taskbar, click the **Windows Explorer** button
2. On the toolbar, click **Organize**, point to **Layout**, and then click **Menu bar**
3. To hide the menu bar, follow the same steps.

Windows Explorer
with the menu bar
visible



Some of the material appearing in this Issue was sent to the editor by other members of the GTBPCUG. Thank you.

Legal Notice

Bay Bytes, Copyright © 2012, is the official newsletter of the Greater Tampa Bay PC User Group, Inc.(GTBPCUG). The information in this newsletter is intended to help our members. It has come from many sources and cannot always be verified. It is recommended that you obtain professional advice from software and hardware distributors, manufacturers, salesmen, or other professionals dealing with the subjects that appear in this newsletter. Unless specifically stated otherwise, the opinions expressed in Bay Bytes articles and columns are those of the individual authors and do not represent an official position of, or endorsement by GTBPCUG. GTBPCUG is not affiliated with any company, vendor or equipment manufacturer. Permission for reproduction of Bay Bytes in whole or in part is hereby granted to other APCUG user groups for internal, non-profit use, provided credit is given to the author, GTBPCUG Bay Bytes along with the copyright notice. Other reproductions require the prior permission of the editor. When published, please send a copy of your newsletter to

editor@gtbpcug.org or mail to P.O.Box 501, Brandon, FL, 33509-0501.