

Founded 1982  
www.rcsi.org



“Your Computer User Group of the Air”, Saturdays from 12:00 pm to 2:00 pm with Nick Francesco, Dave Enright, and Steve Rae. Broadcasting on JAZZ 90.1 FM from Rochester, NY. Call 966-JAZZ (585-966-5299) or 800-790-0415

The RCSI 'Monitor' newsletter can be found in most public libraries in Monroe County. *Free* copies can also be found in the following computer stores: Microworx, Just Solutions, TSC Electronics, and Pod Computers. Digital copies may be obtained from [www.rcsi.org](http://www.rcsi.org) or my cloud storage at <http://tinyurl.com/tonydel-rcsi-newsletters/>.

#### Some Past Presentations:

Open Source and Free Software  
Protecting Your Identity  
Keeping Mobile Devices Secure  
Mobile Payments  
Flash Drives-Not Just for Storage  
Features, Mac OS X & Windows  
Tablets, the Programs and Uses  
Personal Finance Software  
Amazing Browser Tips  
Linux is Like Cars  
Close up Photography



## The Rochester Computer Society, Inc. a computer/tech club open to everyone

# MONITOR

Vol. 35, No. 10

October 2017

Tue, Oct 10, National Cyber Security Awareness Month  
Staying Safe Online, Preventing Ransomware,  
and Identity Theft, by Norbert (Bob) Gostischa

Tues, Nov 14, Customizing & Using Windows 10  
by Hewie Poplock

#### In This Issue

How to Let Someone Else Use Your Computer Without Giving Them Access to All Your Stuff	Chris Hoffman
Double Dose of Ask Leo!	Leo Notenboom
Creating a Backup Image Using EaseUS Todo Free	
Recovering from Ransomware with an Online Backup	
What Instagram is and How to Socially Share Photos	Tech Boomers
Explore Space With This Free Program From NASA	Rob Schifreem

How-To Geek

### How to Let Someone Else Use Your Computer Without Giving Them Access to All Your Stuff

by Chris Hoffman

If you let someone use your computer, they could gain access to your saved passwords, read your email, access all your files, and more. Instead of looking over their shoulder, just use your operating system's guest account feature.

Guest accounts are found on all desktop operating systems—from Windows and Mac to Ubuntu, Chrome OS, and other Linux distributions.



Computer  
and Electronics  
Repair

Custom Computers - Electronic Surplus and Recycling  
Home Service - Small and Mid Size Business IT Mgmt.

765 Elmgrove Rd, Ste 2  
Rochester, NY 14624

Phone (585) 429-6880  
Fax (585) 429-7671

[www.tscelectronics.com](http://www.tscelectronics.com)

## Special Interest Group

### Linux Sig

The workshop is the **third Saturday of each month**, at Interlock Rochester, 1115 East Main St. [www.interlockroc.org](http://www.interlockroc.org)



Enter through door #7 on the end of building, near *Comics Etc* and Goodman St. Find 'Interlock' on the intercom directory to get buzzed in and go upstairs to suite #200. We have experts on hand to fix problems and answer questions about Linux and FOSS (free and open source software). Bring your system in so we can help you get the most out of it. Hope to see you there.

**Free, online  
Virtual Technology  
Conferences,**  
presented by APCUG  
Saturdays from 1-5 pm, on

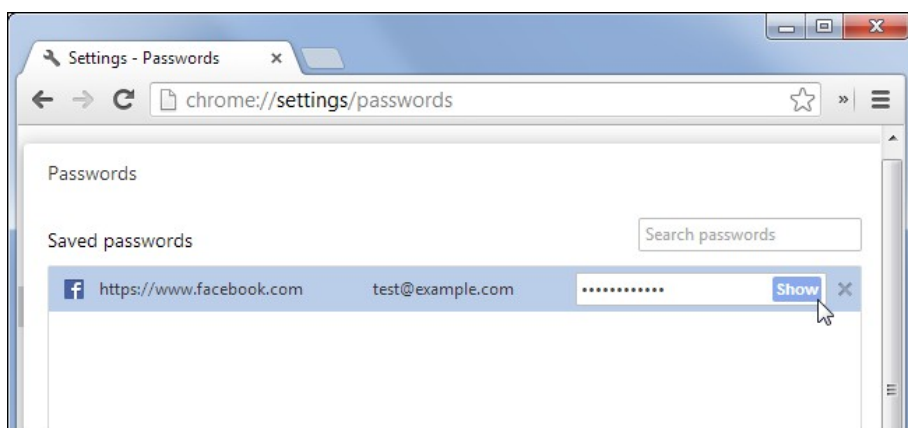
May 6, 2017  
August 19, 2017  
November 4, 2017

The Guest account isn't enabled by default on Windows, so you have to go out of your way to use it.

## Why You Should Use Guest Accounts

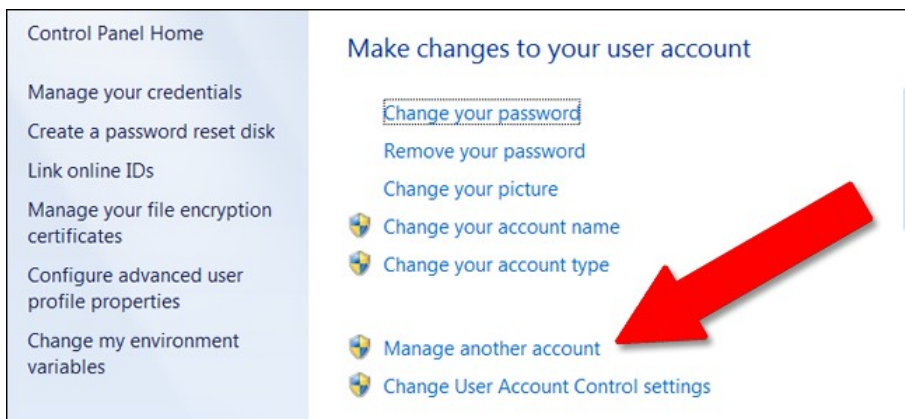
In a previous article, we've covered why it's a good idea to use separate Windows user accounts, and using a guest account is ideal for the same reason. There's no need to create a dedicated user account for temporary guest users. The built-in guest account gives your friend limited access, allowing you to leave them alone with your computer and let them browse the web without giving them access to all your passwords, private documents, email, social media accounts, browser history, and everything else you do on your computer.

Guest accounts aren't able to install software, configure hardware devices, change system settings, or even create a password that applies to the guest account. Guest accounts can shut down your computer—that's about as much harm as they can do.



The guest account allows users to browse the web and use typical applications, so it's a great way to give someone else access to your computer without feeling compelled to look over their shoulder. Even someone you trust may not access your personal data maliciously—they may open your browser, head to Gmail to check their email, and see your inbox if you're already logged in. They'd then have to log out and log into their account, and you'd have to log back into your accounts when they're done. Avoid this headache by using the guest account instead.

## Enabling the Guest Account in Windows



## RCSI Officers

Pres: Steve Staub . . . . . 429-9877

[srstaub1@rochester.rr.com](mailto:srstaub1@rochester.rr.com)

VP: Mark S. Lawson . . . 544-5377

[mslawson51@peoplepc.com](mailto:mslawson51@peoplepc.com)

Treas: Dennis P. McMahon

. . . . . 235-1260

[denmac733@gmail.com](mailto:denmac733@gmail.com)

Secretary: [www.rcsi.org](http://www.rcsi.org)

Help's Half Hour . . Jan Rothfuss

## Board Members at Large

Bob Avery . . . . . 385-4491

[webmaster@rcsi.org](mailto:webmaster@rcsi.org), 9/20

Jan Rothfuss . . . . . 347-6020

[jan\\_rothfuss@hotmail.com](mailto:jan_rothfuss@hotmail.com), 9/19

Tony Dellelo . . . . . 734-6149

[tonydel@techie.com](mailto:tonydel@techie.com), 9/18

## Standing Committees

Linux SIG: . . . Carl Schmidtman

[unixgeek@faultline.com](mailto:unixgeek@faultline.com)

Programs: . . . . . Tony Dellelo

Webmaster: . . . . . Bob Avery

Membership: . . . . . Steve Staub

Monitor editor: . . . . . Tony Dellelo

## Planning Meeting

Held on 1<sup>st</sup> Tuesday of each month  
at 7 pm, at St. John's Meadows,  
Briarwood building.

## Newsletter Printing

The July newsletter was printed at  
St John's/Chestnut Court by the  
printing group, with the help of  
Don Wilder (computer and printer  
operator). We will try and print on  
the 1<sup>st</sup> or 2<sup>nd</sup> Thursday morning,  
following the monthly meeting.

However, we want the account more limited than that. So, we're going to put the Visitor user in the **guests** group. To do this, we must first delete the Visitor user from the **users** group. To do this, enter the following command at the prompt.

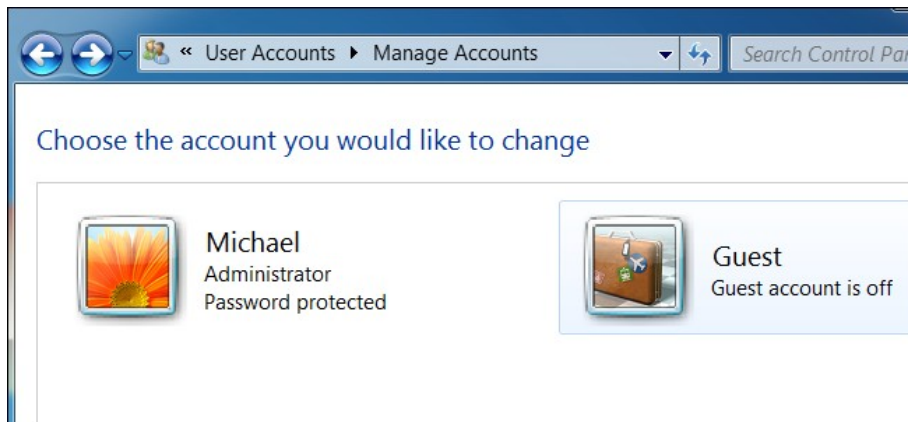
```
net localgroup users Visitor /delete
```

Then, type the following command at the prompt to add the Visitor user to the **guests** group.

```
net localgroup guests Visitor /add
```

Close the Command Prompt window either by typing exit at the prompt or by clicking the "X" button in the upper-

Enabling the guest account is different for Windows 7 and 8 than it is for Windows 10. In Windows 7 and 8, you can enable the guest account pretty easily. From the desktop, click the Start menu and start typing "user accounts." Click on "User Accounts" in the search results. From this menu window, click "Manage another account." Click "Guest." If the guest account feature is disabled, click "Turn On."



Windows 10, unfortunately, hides this feature a bit...partly because Microsoft would like you to exercise a bit of data security, and partly because they'd like everyone to use official Microsoft user accounts. Enabling the guest (or "Visitor" account) requires Administrator access and a bit of command-line legwork.

To open a Command Prompt window, press the Windows key+X to access the Win+X menu and select "Command Prompt (Admin)". You must select the administrator version of the Command Prompt to create a new user account. First, we'll create a guest account called Visitor (you can call it whatever you want). The name "Guest" is a reserved account name in Windows, even though you can't access the built-in guest account anymore, so you'll need to choose a name other than "Guest". To create the account, type the following command at the prompt and press Enter.

```
net user Visitor /add /active:yes
```

Because the Visitor account is so limited, it doesn't really need to be protected. So, we're going to apply a blank password to it, or no password at all. To do this, type the following command at the prompt. The last character is an asterisk.

```
net user Visitor *
```

When asked for the password, press Enter without typing one. Then, just press Enter again when asked to retype the password. By default, new users are placed in the **users** group so they have the permissions for standard users.

right corner of the window. Now, the Visitor user displays in the list of users in the lower-left corner of the logon screen. Guests can simply select the Visitor user and click “Sign in” to log in to the Visitor account and have the use of basic functions like running a browser to surf the web.

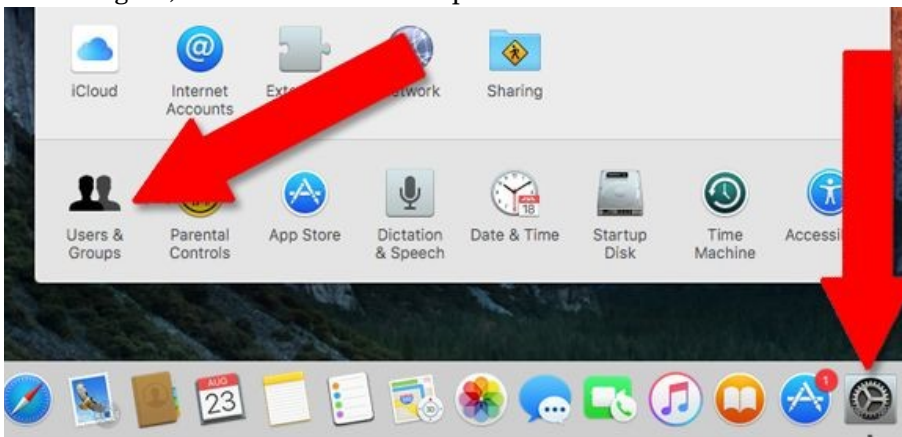
Multiple users can be logged in at once in Windows, so you don’t even have to sign out of your account to let a guest log in to the Visitor account. There are two ways you can access the Visitor account. If you’re currently using your account on the computer, you can select the Visitor account on the Start menu to log into that account for your guest. If the screen is locked, the guest can click on the Visitor account on the logon screen. While the guest is logged into the Visitor account, they can see that you’re logged in, but if they try to get to your account, they will be asked for your password on the login screen. If you find you don’t need it anymore, you can delete the Visitor account, just like you can any other user account.

Once they’re done, they can log out of the guest account. Note that their browsing history, logged-in websites, and any other files or data they left lying around will remain accessible to future users of your guest account. Guest users should log out of any websites they accessed or just use a browser’s private browsing feature inside the guest account.

If you’re worried about what files the guest user can access, feel free to log in as the guest user and poke around. By default, files shouldn’t be accessible as long as they’re stored in folders under your user folder at C:\Users\NAME, but files stored in other locations like a D:\ partition may be accessible. You can lock down any folders you don’t want guests to have access to with the security properties dialog. If you like, you can also rename your Windows guest account.

### Enabling the Guest Account in macOS

On a Mac, you can log in as the guest user by selecting the Guest User account on the login screen. If this option isn’t available, you’ll have to enable it. From the desktop, click the System Preferences icon in the dock (the one with the gear). Click “Users & Groups”.



Click the lock icon in the lower-left corner, then enter your administrator password to access advanced functions.

**Articles by RCSI members may be reprinted by other user groups**, without special permission, provided they are unaltered and the publication emails a copy to the author. Articles by authors from other organizations retain their original copyright. Articles provided by the Association of Personal Computer User Groups (APCUG) may be reprinted if credits remain intact.

### Computer Recycling

Some Residential Drop off  
Locations: **Call first**, to find out what is accepted, especially for 'tube type' tvs or monitors.

### Monroe County *ecopark*

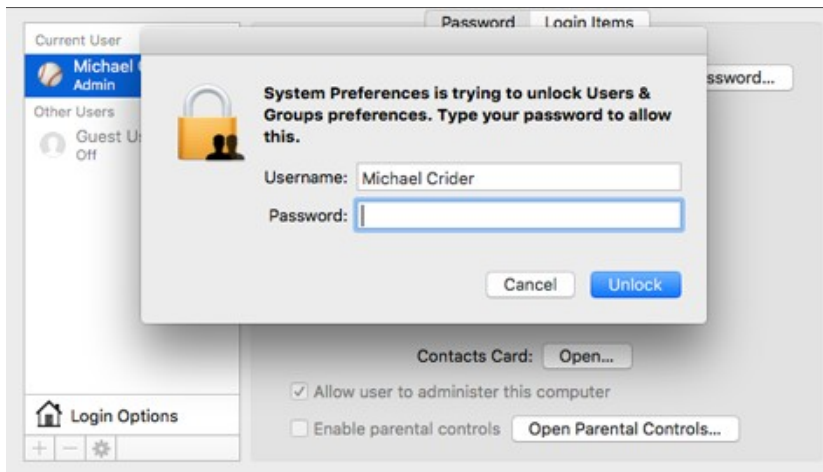
(Cathode Ray Tube TVs and monitors - \$10 each credit/debit card only) 10 Avion Drive  
Rochester, NY 14624  
Phone: (585) 753-7600 (Option #3)

**Best Buy** stores accept most electronic waste (CRT and some other TVs include a fee of \$25 each)

**Maven Technologies** offers *free* residential drop off, 9:00 am – 4:00 pm (M-F), 1450 Lyell Avenue, Rochester, NY. The processing center is located on the NW corner of Lyell and Mt Read, behind the 'strip mall'. Go to the customer entrance. 458-2460.

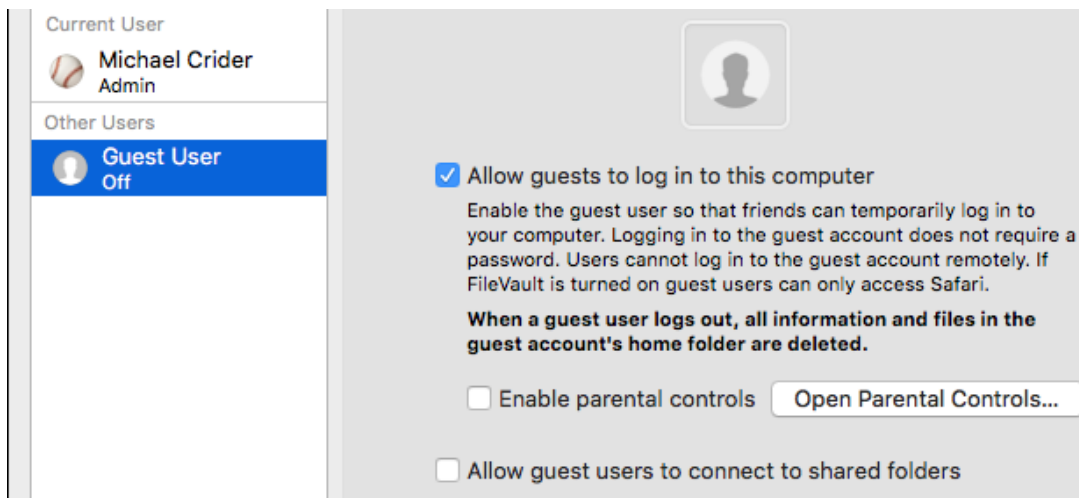
**Pod Computers** accepts most electronic waste (no tv's or crt's), located at 1925 South Ave, the wedge where South Ave and East Henrietta Rd meet. 244-2240.





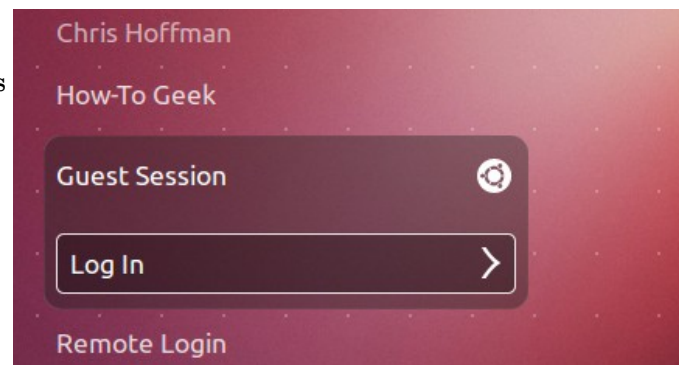
Click “Guest User”, then click the check box next to “Allow guests to log in to this computer”. Don’t click “Allow guest users to connect to shared folders”, unless you want to give them access to your personal files.

Log out. You’ll now have a guest user account accessible without a password. Once your guest logs out, all their data will be erased (unlike Windows).



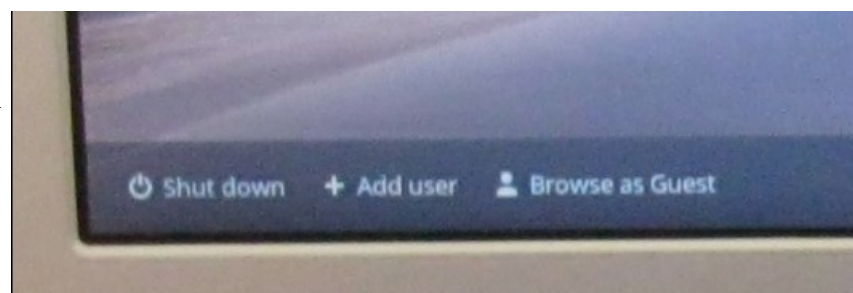
### Using the Guest Account on Ubuntu

On Ubuntu, the guest account is enabled out of the box. You can select the Guest user on the login screen to log in as the guest account. Like macOS, all their data will be wiped when they finish and log out of the guest account.



### Using the Guest Account on a Chromebook

Google's Chromebooks also offer a guest mode. Like macOS and Linux, all guest user data will be automatically wiped when the guest user logs out.



Article is from the [www.howtogeek.com](http://www.howtogeek.com) website. I took some editorial liberties and combined some information from another article by Chris Hoffman.

## Linux Workshop, 3<sup>rd</sup> Saturday of each month, Noon-4PM

Interlock Rochester, <http://www.interlocroc.org>

**1115 E Main St, Suite #200, 2<sup>nd</sup> floor** (enter through door #7)

Come and get your questions about Linux answered. We have experts on hand to fix problems and answer questions about Linux and FOSS. Bring your system in so we can help you get the most out of it.

1115 E Main St is at Goodman Ave - the Hungerford Bldg. Find Interlock on the buzzer menu next to the outside door. Go up stairs.

Ask Leo !

By Leo Notenboom, <https://askleo.com/>

**Making Technology Work For Everyone**

## Creating a Backup Image Using EaseUS Todo Free

Microsoft is apparently removing image backup capability from Windows 10. We'll make an image backup using a third-party alternative.

//

Apparently, Microsoft has decided to pull the plug on image backups (known as the “Windows 7 [Backup](#)” tool in Windows 10). My current understanding is that it is at least “deprecated”, and will likely actually be removed from a future Windows 10 update. This will leave Windows 10 with no built-in [image backup](#) capability of its own.

The official word from Microsoft is that third party utilities should be used instead. This doesn't break my heart, as I was never a fan of the tool. I had hoped, however, that they would improve, rather than remove, the facility.

EaseUS Todo is a backup program whose free edition is superior to Windows' built-in tool. I'll show you how to create an image backup using it. The bonus is, this is not limited to Windows 10 at all; as of this writing, the free edition works with Windows XP, Vista, and all versions of 7, 8, and 10.

### EaseUS Todo

EaseUS Todo can be downloaded from their website. (As always, I strongly recommend avoiding “[download](#)” sites” and getting software directly from the manufacturer whenever possible.)

There are three things to note about the download and install.

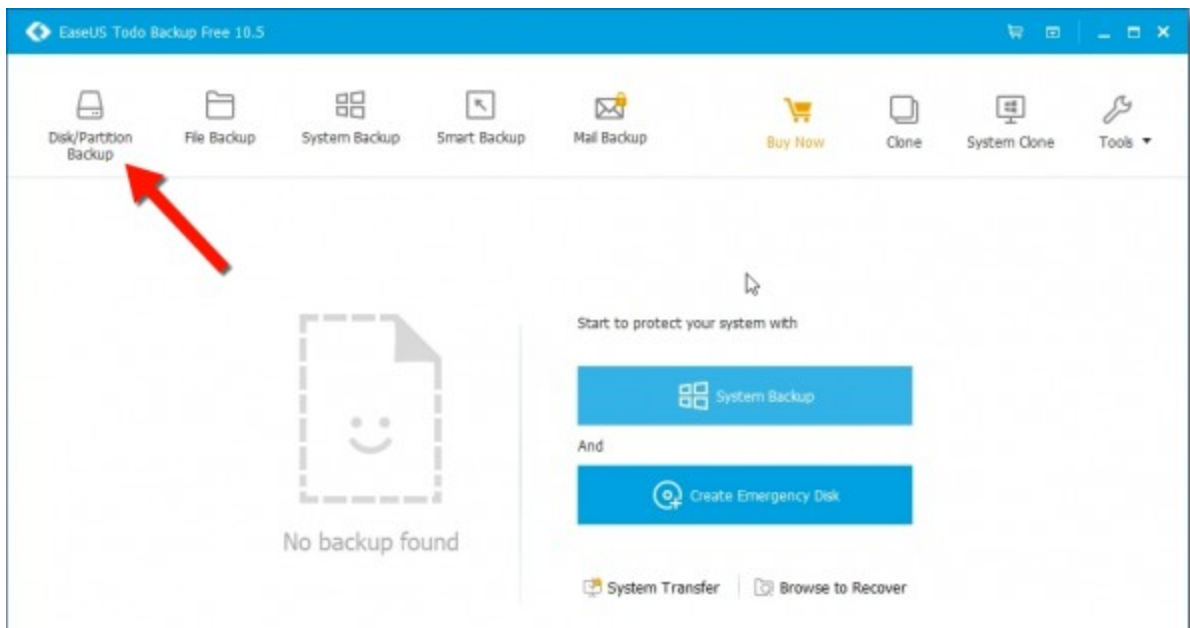
First, you will be *repeatedly* offered the opportunity to choose their retail product, or a trial version of their retail product. These products are not free. They're also not needed for what I'm about to show you. Sometime later, you can return and upgrade to one of their paid offerings if you like. Be very careful, and make sure you always and only choose the truly FREE version of EaseUS Todo.

Second, you will be asked for an email address. In a sense, this is the “cost” of the free edition. I have no complaints with EaseUS email, and you can always unsubscribe later. They do frequently offer discount codes for their retail product, so if you think you might be purchasing at some point in the future, it's worth getting on their list.

Finally, like most free software, be on the watch for [PUPs](#) (Potentially Unwanted Program). EaseUS does not hide the additional software offered with Todo, but it is selected by default. Be sure to deselect it during the install process.

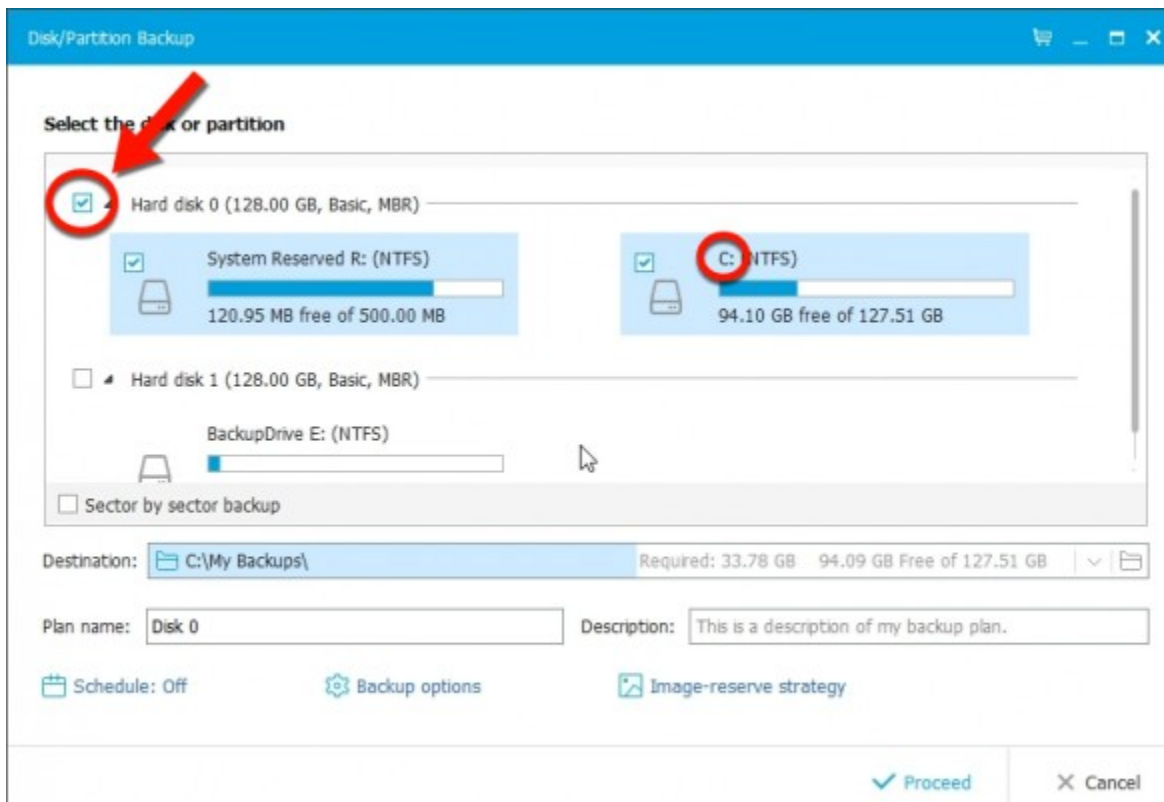
### Creating an image

Run EaseUS Todo, and on its main screen, click on **Disk/[Partition](#) Backup**.



I choose this over “System Backup” or “Smart Backup” because it provides explicit control over the disks and partitions included in the backup image.

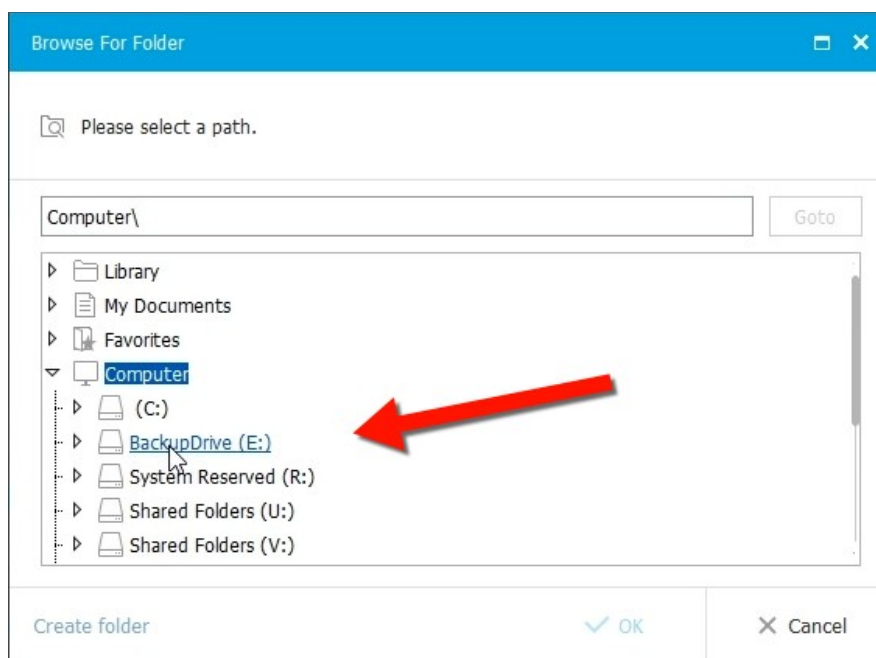
On the resulting screen, check the box to the left of the disk that contains your system or C: partition. This will ensure that the entire [hard disk](#) that contains your system, including any additional partitions (such as recovery partitions), will be included in your backup.



Next, click on the small folder icon to the far right on the “Destination:” line.

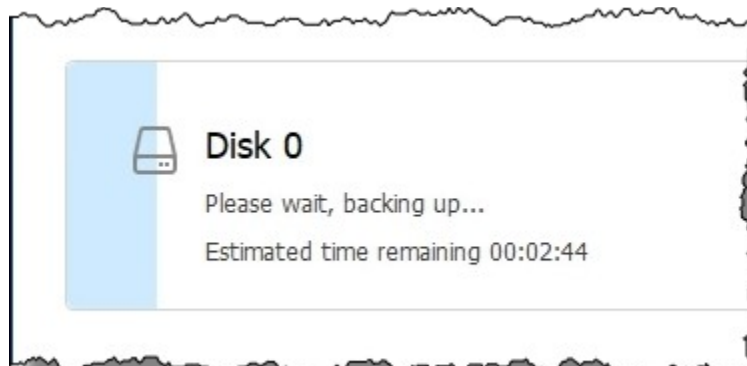


This will open a folder selection [dialog box](#). Use that box to select the destination: the folder, typically on your external hard drive, into which the image backup is to be placed.



Click **OK** to accept your selected destination folder.

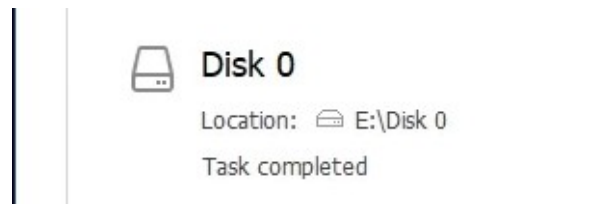
Click **Proceed** to begin the backup.



Naturally, this will take some time. Exactly how long will depend on the speed of your system, the speed of your hard disks, the amount of data to be backed up, and more. I will point out that EaseUS Todo’s “Estimated time remaining” indicator is notoriously inaccurate.

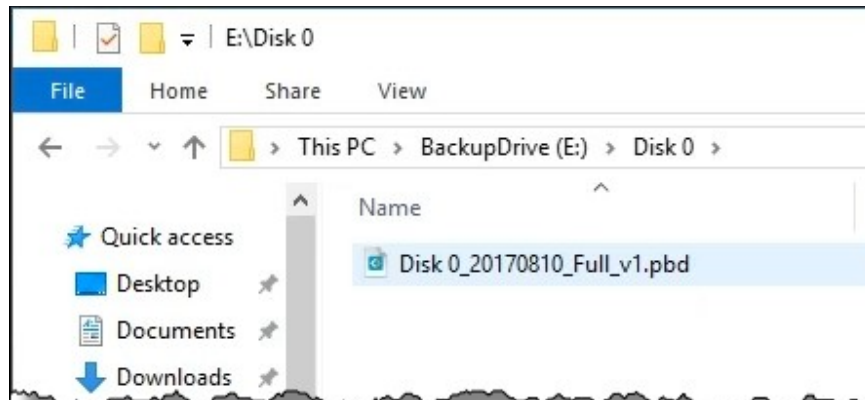
### Your backup image

Eventually, the backup completes.



Open Windows File Explorer and navigate to your previously selected destination, and you should find a “.pbd” file.





That file contains the image backup of your system.

\*\*\*\* End of article.

Ask Leo !

By Leo Notenboom, <https://askleo.com/>  
**Making Technology Work For Everyone**

## Recovering from Ransomware with an Online Backup

People often cite ransomware as a reason to avoid automated online backups, thinking that those backups will be impacted. OneDrive provides an answer.

//

One of the comments I quickly received on my article [“Using OneDrive for Nearly Continuous Backup”](#) was this:

If one should fall victim to hostile file [encryption](#), instantaneous [backup](#) to OneDrive presumably would result in those being encrypted too.

In other words, if you’re using OneDrive (or Dropbox, or other similar services) to automatically [back up](#) files online whenever they change, doesn’t that mean that [ransomware](#) would cause those backups to automatically be replaced with their encrypted versions?

Yes.

But before you give in to a knee-jerk reaction to avoid online backups completely, consider this: they’ll give you more options, not fewer, should ransomware ever strike. In fact, they could save you in ways other backups might not.

### Online backup to the rescue

Whenever a file is deleted from your computer in a folder being [continuously backed up by OneDrive1](#), the following happens:

- Any prior copy of the file is *moved to a Recycle Bin* on the OneDrive servers.

Whenever a file changes on your computer in a folder being [continuously backed up by OneDrive2](#), the following happens:

- The prior copy is moved to the version history for that file. (A kind of recycle bin specifically for that file.)
- The new copy is uploaded.

Yes, [OneDrive has a Recycle Bin](#). This means *OneDrive can save your data from ransomware*.

It would work like this:

- You use [OneDrive to keep a more-or-less continuous backup](#) of your data online.
- Your machine becomes infected with ransomware of some form, and all your data files are encrypted (and therefore lost to you).
- If you are online, OneDrive dutifully notices that the files have changed, and backs up the now-encrypted files.

- You panic. (Technically, this step is optional, but quite common.)
- You disconnect, clean up, rebuild, or otherwise remove the malware from your machine, but are left with all of your files encrypted.
- You visit OneDrive online, and recover your *unencrypted* files from its Recycle Bin and each file's version history.
- You vow to never again do whatever it was that allowed the malware infection to happen in the first place.
- Life goes on.

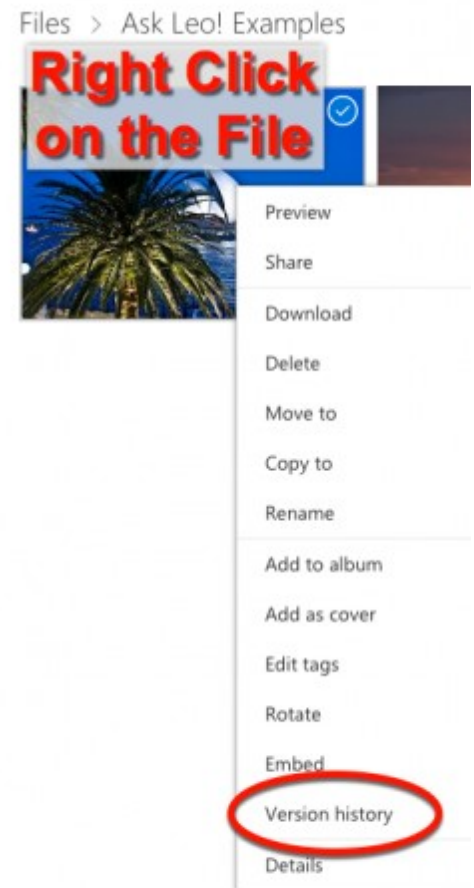
OneDrive just saved your bacon. What's more, everything I've described above all happens without any other form of backup in place. But of course, you also have other forms of backup — right?

### Belt and suspenders and suspenders

The person who originally left the comment continued:

“A simple, but probably inefficient, means I use is to weekly make a copy within OneDrive of backed up files”.

This is (almost) *exactly* what I do myself. Every night I make a copy, elsewhere on my machine, of everything in my OneDrive folder, in the form of a compressed archive (like a “.zip” file). Should I ever succumb to ransomware, I can recover my files from that additional backup. I would not make the copy “within OneDrive”, however, since ransomware could impact that backup copy as well. Of course, on top of that, I have my nightly backups running to an external hard drive: monthly full backups with daily incrementals, meaning I can always recover the files “as of” a few days ago. (And in case I happen to run across ransomware that also tries to encrypt backups ... some of those backups are copied elsewhere, effectively “offline” and not directly accessible to my machine.) It would take a lot for even the nastiest ransomware to cause me to lose any significant number of files.



### You don't need to go overboard

You don't need to be as backup-crazy as I am. You can protect yourself with just a few simple steps.

- [Use OneDrive for nearly continuous backup](#) of your day-to-day working files.
- [Enable File History](#). File History, though sometimes disabled by more aggressive ransomware, will also let you [restore a file](#) to the condition it was in prior to encryption, and can protect files outside of those you keep within OneDrive.
- Take [periodic full, and more frequent incremental](#), image backups of your entire system to protect from almost any type of failure.
- Every so often, take one of those full backup images and copy it to offline storage.

And, honestly, that last one is just to make people panicking about ransomware encrypting their backups happy. That doesn't happen so often that I consider it truly critical, particularly with what we've just discussed about OneDrive's Recycle Bin.

### Don't let the worst case scare you away from reasonable choices

What concerns me most are folks who say they won't use online backups because their files *might* be encrypted by ransomware and the online backup would be useless.

Ransomware is only one type of threat. More importantly, it's not even the most likely threat.

For example, a [hard disk](#) failure can be *much* more destructive than ransomware, and is probably much more likely to happen. Even more bluntly: you're more likely to accidentally overwrite or delete a file than you are to personally encounter ransomware.

Even if the Recycle Bin didn't exist, continuous online backups save your files from many threats that *don't* involve

invalidating the backup.

The same is true for nightly backups to an [always-connected external hard drive](#). Yes, there's a chance that ransomware could encrypt your backups. There's a higher probability that you'll be glad you had those backups current for a variety of other failures.

Making backups easy, timely, and automatic is more important than fearing one specific — albeit destructive — form of malware.

\*\*\*\* End of article

\* \* \* \* \* SOFTWARE and HARDWARE \* \* \* \* \*

TechBoomers

## What Instagram is and How to Socially Share Photos

Have you ever created a photo album, or wanted to make one? What if you could easily make a virtual one online? What if it could contain photos AND videos? What if you could capture a photo or video, edit it, throw in some creative touches, and add it to your photo album right on the spot? And what if you could show your photo album to all of your friends and family over the Internet?

If any of that sounds interesting to you, then you're in luck! There's an app for your smart phone or tablet computer called [Instagram](#), and it can do all of these things! What's more is that it's so simple to use that many celebrities have their own accounts. Popular users include musicians/singers like Beyoncé, athletes like Lionel Messi, and movie and television stars like Ellen DeGeneres.

### What is Instagram?

Instagram is an easy-to-use mobile application that lets you capture and edit photos or videos on your tablet computer or smart phone. You can then share your creations on Instagram and various other social media websites, such as Facebook, Twitter, and Foursquare.

### Why use Instagram?

You should use Instagram because it's an awesome multi-purpose app. It was initially designed to support social networks, but it has since become a social network all its own. Users can follow what other users post, or leave a "like" or comment on a photo or video that they find interesting.

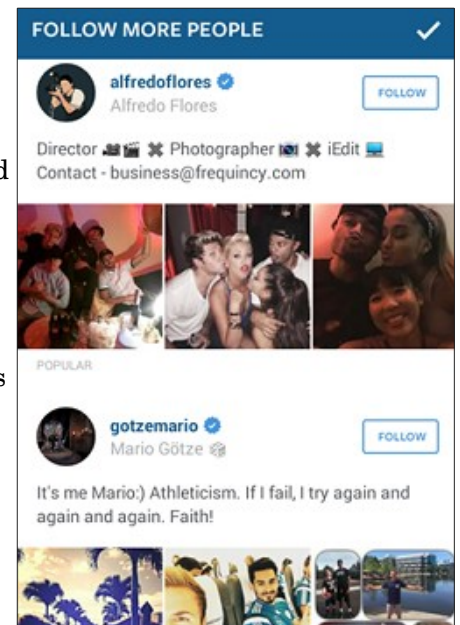
If you feel like being more private, users can require approval before other people are allowed to see their posts, or send posts privately to specific other users with the "Instagram Direct" feature.

### How does Instagram work?

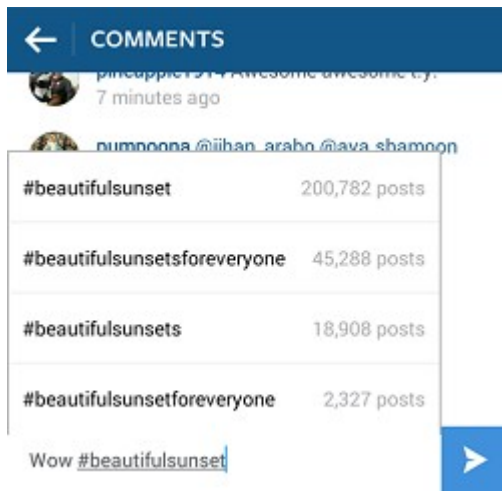
Instagram works as a photo and video editing tool, as well as a stand-alone social networking app. You can also use it to simultaneously share photos and videos across multiple social media platforms, and if you're a business owner, as a tool to promote your business. Let's go over 5 ways Instagram works.

#### 1. Make connections with other users.

Many other people use Instagram, from celebrities and corporations to budding photographers and blog enthusiasts. Some users may be your friends or family! You can connect with them and follow what they do, and they can do the same for you.



## 2. Show off your visual media creativity by sharing unique photos and videos.



You can put photos and videos already on your mobile device on Instagram, or you can use the app to take a new photo or record a new video. After that, you can use filters and other effects to give a unique look to your creations!

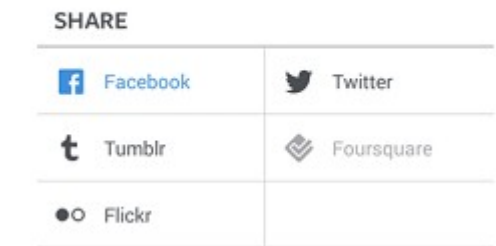
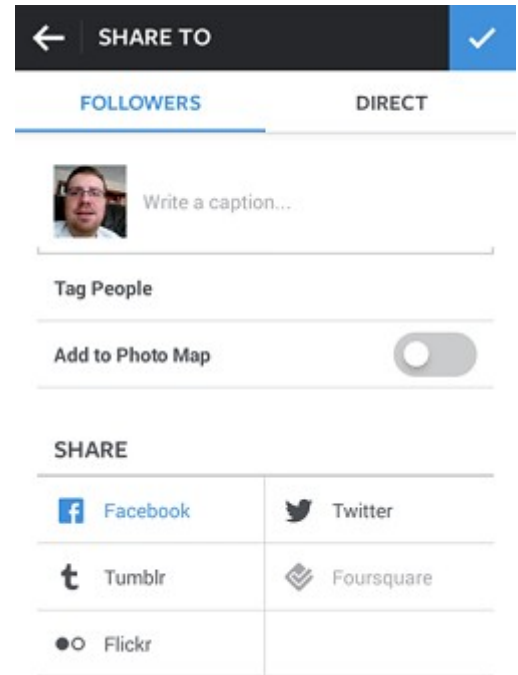
## 3. Organize and categorize all of your posts to make them easier to find.

Instagram supports the use of "hashtags," which are short words/phrases/abbreviations preceded by the "#" sign that you can add to your posts to help categorize them. This not only makes them easier to find for you, but it also helps other people find them as well!

## 4. Share your posts across multiple social platforms.

Why just stop at sharing your photos and videos on one social network? Instagram allows you to connect to many other social networks, which means that you share photos and videos on Instagram and your other accounts all at the same time!

## 5. Change your account from "social" and "personal" at your leisure.



Are you the shy type who would rather use Instagram as their own private online photo album? No problem! You can set your account to private, which means that only people whom you approve as "followers" can see what you've posted. You can also use "Instagram Direct" to send a private post to a friend that only they can see, so it won't show up in any public place on Instagram.

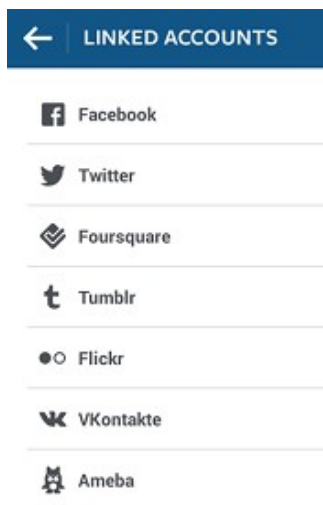
If Instagram sounds like something you think you'd love, don't forget to download it from the [App Store for your Apple device](#), or the [Google Play](#)

[store for your Android](#).

## 4 Ways to Use Instagram

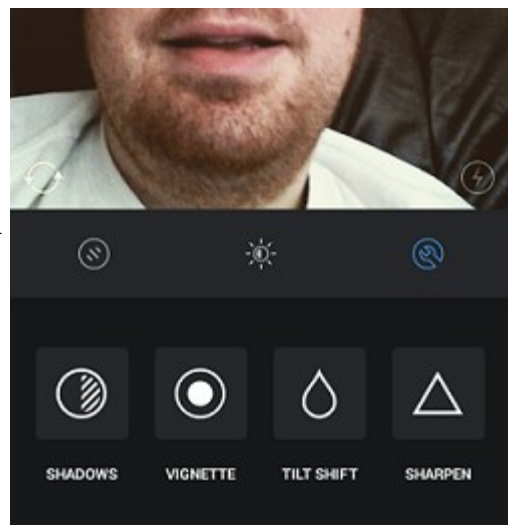
### 1. Use Instagram to capture photos and videos, and as an editing program.

You can choose to upload photos or videos that are already stored on your mobile device or tablet, or you can capture photos and videos from within the Instagram app. The app also gives you the tools to edit your photos and videos. You can add cool filters to give a unique effect to your photo/video, or use the more advanced tools to further modify your photos before sharing them.



### 2. Use Instagram to share photos and videos across all your social media platforms.

You can connect your other social media accounts to your Instagram profile so you can





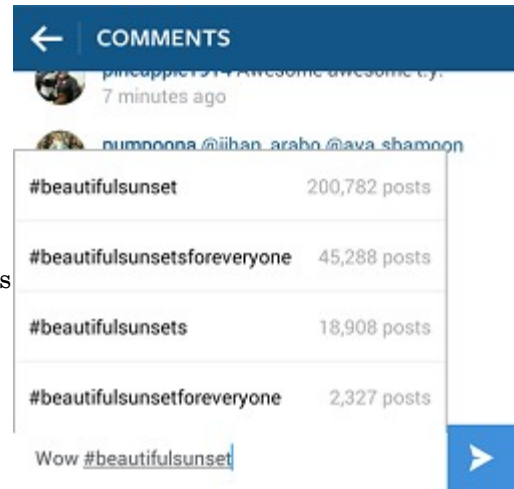
instantly share the same post across all of your social networks. Some of the social networks that Instagram can connect to include Facebook, Twitter, Tumblr, and Foursquare. After you've linked your other social networks to your Instagram account, you can use it as a tool to share one post across all major social media platforms. When you're about to share a photo or video to your Instagram page, you can instantly share it across your other social networking accounts simultaneously.

3. Use Instagram as a social network to stay connected with your friends, family, and other users.

You can use Instagram as a social network on its own. You can follow other users to see their posts on your timeline, and others can follow your posts as well. You can choose to follow your friends and family, your favourite celebrities, and your favourite brands. You can "like" other users' posts, or leave them a comment to let them know what you think! Similarly to Twitter, you can use "hashtags" to categorize your posts according to their topics, or "mention" other users to connect them to your posts.

4. Use Instagram as a tool to promote your business.

Lots of companies are now using Instagram as a way to promote themselves. Brands, companies, organizations, and businesses can create their own Instagram pages to promote their products and services. It's a great way for companies to gain exposure, show off what they've been up to, or show sneak peeks at what they have in store for their customers!



## History of Instagram and why it's so popular

Instagram launched in 2010, and within one week had over 100,000 users. Three months after launching, Instagram hit 1 million users. The popularity and user-base of it grew rapidly from the very beginning, and has not stopped since.

In the beginning, the idea behind Instagram was to provide users with a way to communicate through images. It has since blossomed into a multi-media social network. As it grew, the company was acquired by Facebook in 2012 for around \$1 billion. Since being purchased by Facebook, many features have been added to Instagram, such as direct messaging and live streaming. Instagram, like Facebook, is now more of a one-stop social network with 600 million monthly active users.

Instagram is so popular because it gives users a way to capture, edit, and share photos and videos within the app itself, as well as across other social media platforms. Instagram gives people a way to stay connected with their loved ones, and to stay up to date with their favorite celebrities as well.

## How safe is Instagram?

Instagram is just as safe to use as other popular social networks. As long as you don't violate their terms of service, or do anything careless, you'll be safe using Instagram. If you're concerned about your privacy, you can set your profile to "private" so you can decide who can follow you and see your posts. If you'd like to learn more about how to stay safe using the app, check out our article on [Instagram safety](#).

## Instagram pros and cons

There are lots of reasons why Instagram is a great app to use, but there are also a few things that aren't so great about it. Let's go over a few of the pros and cons to help you decide whether or not it's right for you.

First, let's start with the pros. Some of the great things about Instagram are that you can capture, edit, and share photos and videos, all within the app, and all for free! You can choose from a variety of filters and built-in editing tools to give your photos a unique look. You can decide to share your posts with everyone, or set your account to private if you'd rather keep them to yourself. Tons of people use Instagram, so you'll be sure to find other users to follow as well!

Some of the not so great things about Instagram are that it's designed for mobile devices, so you can't post from your computer (without the help of a third-party app). Also, since all of its services and features are free, they sometimes show advertisements in your feed.

## Instagram competitors

If Instagram isn't quite right for you, don't worry – there are other similar apps and websites you can use instead. If you're more interested in photo editing features than social networking features, try out [VSCO.co](https://www.vSCO.co) or [Pixlr.com](https://www.Pixlr.com). If you'd feel more comfortable using a photo-sharing service that's been around for a long time, try out [Flickr.com](https://www.Flickr.com). If you're looking for a unique social media network that includes photo and video sharing as part of its platform, check out [Path.com](https://www.Path.com) or [Galaxia.co](https://www.Galaxia.co).

you want to learn more about the app and how to use it, we'll show you the ropes! Check out the rest of our [Instagram course](#), where we'll walk you through getting the most out of Instagram – installing it on your device and setting up an account, to producing, organizing, and sharing your photo and video creations. Read on to become an Instagram pro today!

Taken from the TechBoomers website [www.techboomers.com](http://www.techboomers.com), April, 2017.



**POD Computers**

**1925 South Ave.**  
Corner of South Ave. and  
East Henrietta Rd.

**244-2240**

**What we do**

- Windows, Mac, and Linux
- PC Repair
- Mac Repair
- Virus Removal
- Custom System Builds
- Data Destruction
- Electronics Recycling

Laptops starting At **\$129<sup>99</sup>**

Desktops starting at **\$149<sup>99</sup>**

**Rochester Computer Society**  
Members receive 10% off  
(must have membership card to redeem)

[www.podcomputers.com](http://www.podcomputers.com)



Gizmo's Freeware

## Explore Space With This Free Program From NASA

by Rob Schifreem

Ever tried Google Earth to look at some local or distant streets, and wondered whether it's possible to do the same thing with outer space? Well, it is, and the technology comes from NASA and the Jet Propulsion Laboratory, so this isn't some amateur offering. Instead, it's a superb way to explore the solar system, planets and exoplanets, as well as earth and the satellites that currently orbit it.

It's a fascinating and educational tool, which is available for Windows and other platforms too. The initial download is around 50 MB, but be aware that it will then download a lot more additional data and graphics from NASA's servers. So you'll need a decent internet connection in order to make use of it.

NASA's Eyes, as it's called, is free and you'll find it at <https://eyes.nasa.gov/>. The installer is malware-free according to VirusTotal, and the site is rated as reputable by Web of Trust.

Article is from [www.techsupportalert.com](http://www.techsupportalert.com) website, specializing in finding free quality software.

