TeamViewer

By Joel Ewing, President, Bella Vista Computer Club, AR
February 2018 issue, Bits & Bytes
http://bvcompclub.org
president (at) bvcompclub.org

One way to get help with a computer problem or with a problem using a particular application on your computer is to physically take the computer to an expert or get an expert to make a house call.

If the computer is sufficiently functional and is connected to the Internet, another alternative may be to allow an expert to remotely connect with your computer to diagnose and fix the problem by controlling your computer remotely. One utility that may be used for this purpose is TeamViewer, free for personal use and available from https://www.teamviewer.us/solutions/remote-access/

Some of the BVCC personnel who provide help at our Help Clinics are also willing to provide help remotely via TeamViewer.

TeamViewer allows one computer to remotely view and control a remote computer using a secure encrypted connection over the Internet or over a local network: it's as if the remote operator were sitting in front of your computer viewing your display and with access to your keyboard and mouse. You run an appropriate version of TeamViewer on both the controlling system and the target system. There are versions that run on many different platforms and environment types: Windows PC, Linux PC, Mac, and Mobile Devices are all supported. The Windows version is compatible with Windows versions XP (SP3 level), Vista, 7, 8, 8.1, and 10. The Windows XP and Vista support does additionally require IE8 or later to be installed. The Linux version in some cases may support outbound connections (to control a remote system) but not inbound connections (to be controlled).

There are several ways in which TeamViewer may be used. The way we are recommending requires users at both machines to start TeamViewer when a specific remote diagnostic session is to be established with a known party. When started, TeamViewer will display a 9-digit numeric ID unique to that machine and a numeric password that should be different each time TeamViewer is started. The user at the machine that is to be remotely controlled communicates by phone his ID and password to the other user to give access to his machine. When the remote user enters the ID and password, a session with the remote computer is established. The connection creation requires use of an Internet server operated by TeamViewer, which uses the ID to link to the target machine, and then the target machine verifies the password. If possible, a direct encrypted connection between the controlling and controlled systems will be established; otherwise, the TeamViewer server will serve as a relay point, passing encrypted data between the two machines.
Another way in which TeamViewer may be used is to configure it for unattended operation: have TeamViewer start up with Windows and run with a known password so

it may be accessed without a person present. The intent is that you would be able to access your own computer from a remote mobile device, but it also means that anyone else who might discover your ID and password could connect to your system and compromise it without you being aware. We are not recommending that type of usage, because it is possible to choose options that may unnecessarily put your system at risk for abuse over the Internet.

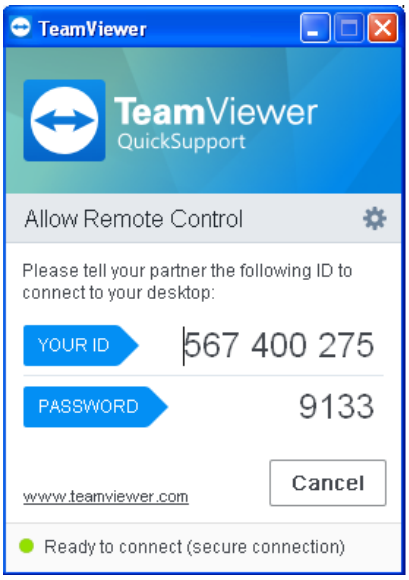
If you are sitting in front of your computer, you can see when someone has access via TeamViewer and act to terminate the connection if you did not authorize it. If the connection is by someone you didn't intend or expect to have access and it occurs when the computer is unattended, it would be trivial for that person to install any variety of malware on your system without your knowledge.

Although TeamViewer's security protocol appears technically sound and they are clearly a security-conscious business, their server platform must somehow store the ID codes for millions of TeamViewer users, making that server an attractive target for hackers, and no site is guaranteed 100% secure 100% of the time when humans are involved. Should your ID become known, a 4-digit password will not keep your system secure for long if your system is always up, with TeamViewer always active, and with a short, fixed password. Your own usage of TeamViewer to access your home site from a remote mobile device could also become an exposure. Should that mobile device become infected with malware and compromised, your TeamViewer ID and password could also be compromised, making it easy then to compromise your home system as well.

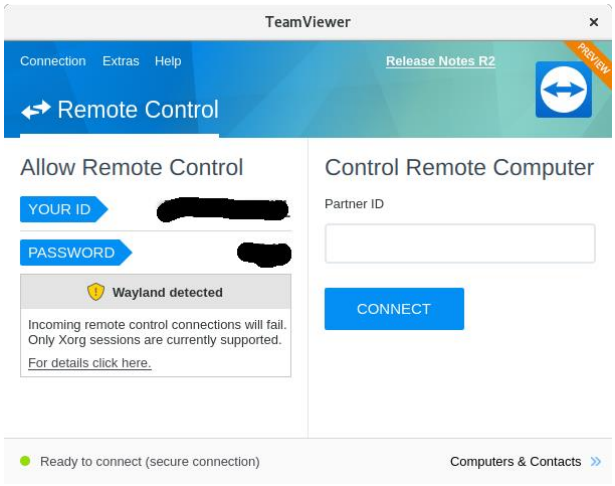
So how do you install free TeamViewer for personal use? Go to the TeamViewer site given earlier, select "Download Now", indicate when asked that your intent is "To access my personal computer at home" (personal, rather than business use). You should be taken to the download page appropriate for your Operating system type. In the case of Windows, you can choose the "Download TeamViewer" button to download a full version of the program that can be installed on your system, or you can choose the "Download QuickSupport" button to download a smaller version that can be executed without installing to allow your system to be remotely controlled for diagnostic assistance only. Alternatively, you can use versions supplied by BVCC Help Clinic personnel.

The simplest and most secure way to execute TeamViewer for a remote diagnostic session is to just download and execute the TeamViewer Quick Support version, which does not support the always-up options that could be mis-configured to make your system more vulnerable. If you execute the TeamViewer QuickSupport version, when it starts you will see a screen like the following:

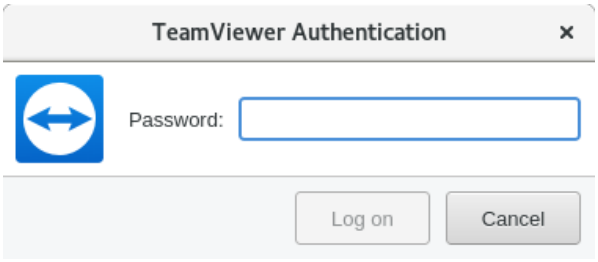
(This is from a virtual Windows system that will be destroyed after writing this article, so it doesn't matter that ID & Password are revealed.)



On a second system that will be used to control the first and where the TeamViewer application is installed, executing TeamViewer displays:

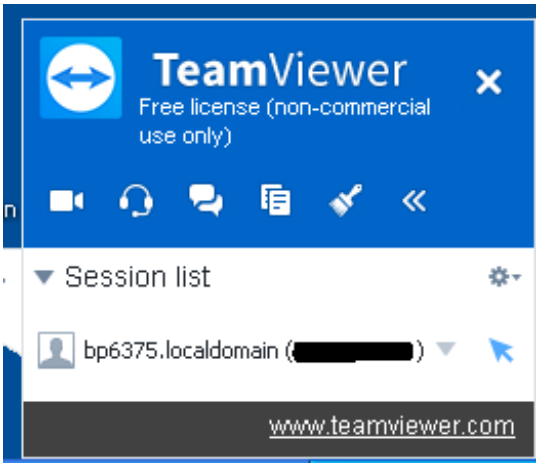


If on that machine you key into the Remote Computer "PartnerID" field the ID of the first machine, you will next be asked for the password.



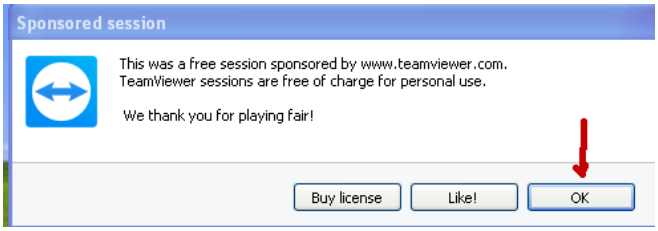
and if the password of the first machine is correctly entered, the second machine will now display the desktop of the first machine and will be able to control that machine. The first machine will show that it is being remotely controlled by displaying a desktop window on the bottom right including the name and ID of the controlling machine

(I blacked out the 9-digit ID). Closing that window on the controlled machine is one way to break the controlling connection. While a connection is in effect, it is possible for the users at the controlling and controlled computers to text via a Chat feature in TeamViewer and mark on the controlled desktop as a means of communication, but most cases, it would be more efficient to communicate by phone on a speaker phone. There also appears to be support for handling video conferencing between the computers, but this presumes both systems have a functional microphone and camera, which mine do not.



in

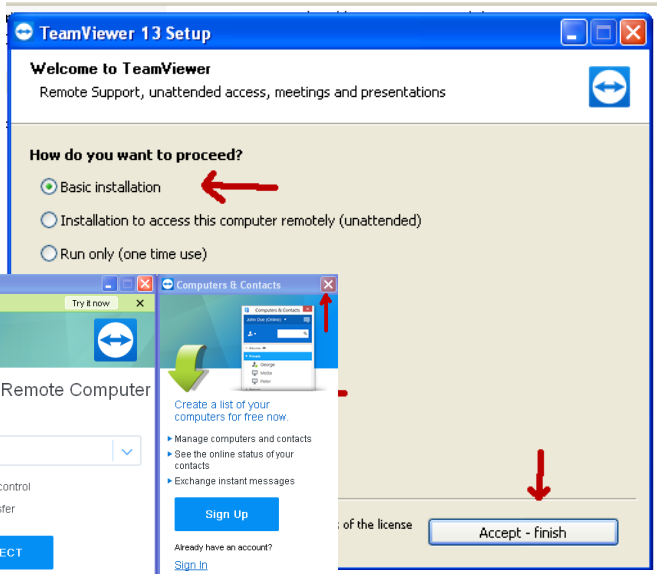
When the TeamViewer session is terminated, you will get a window reminding that you are using a free version for personal use only. If you are not using it to support a business, the correct response is “OK”.



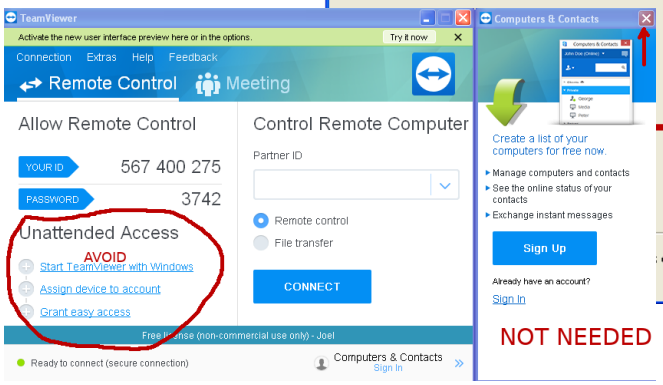
After closing that window, you will get one more advertisement for purchasing a business license, which should be ignored for personal usage. Another useful feature which is available if both operating systems are some variety of Windows is to initiate a File Transfer session rather than a Desktop Control session, so files can be moved between the two computers. When running in this mode, the controlling system displays a window similar to those of FTP client applications, where the left half is local machine files, the right half is remote machine files, and you can search directories and drag-drop files from one machine into the directory structure of the other. Unfortunately, if you are primarily a Linux user, this feature isn’t functional with release 13 when one of the machines is running Linux instead of Windows (at least in the case where the Linux system doesn’t support in-bound TeamViewer connections). There are other TeamViewer features related to meetings and conferencing that I didn’t explore, because they weren’t relevant to its remote diagnostic capabilities.

If you choose in install the full TeamViewer version rather than just run the QuickSupport version., there are install options you need to avoid.

Specify “Basic” (not unattended access) and that installation is for “Personal” use, and “Accept”.



The first time the program is opened, at least on the Windows install pictured here, you will also have a Computers & Contacts window as shown.



If you only plan to use TeamViewer to allow a technician to remotely control your system for problem diagnosis, then you don’t need an account with TeamViewer & Contacts window and the Computers can be ignored and closed. The main window also enables you to turn on various features that support unattended access. Unless you have a really good reason why you need this capability, don’t activate it, because it increases the risk that your

computer might be exposed to malicious damage over the Internet should your ID and password become compromised.

If you must have TeamViewer configured for unattended connections, there are recommended option combinations that should be researched and observed. Option settings may be found under Extras → Options. It's probable that installing with "Installation… (unattended)" rather than "Basic Installation" will set a combination of options that are within recommended guidelines for unattended access, provided adequate passwords are used, but I have not attempted to verify this.