Bits & Bytes

Arkansas' Premier Computer Club

December 2021

Bella Vista Computer Club - John Ruehle Center

Highlands Crossing Center, 1801 Forest Hills Blvd Suite 208 (lower level), Bella Vista, AR 72715

Website: http://BVComputerClub.org **Email: editor@bvcomputerclub.org**

MEETINGS

Board Meeting: December 13, 6pm, in John Ruehle Training Center, Highlands Crossing Center.

General Meeting: December 13, 7pm, "Computer Basics", presenter Joel Ewing. Puzzled, confused by all those terms used to describe the capabilities of a computer? This will be a return to basics: what many of those terms mean and an overview of how computers do what they do.

We will meet in-person in Room 1001 on the lower level of The Highlands Crossing Center, 1801 Forest Hills Blvd, Bella Vista, or you may attend the meeting on-line via Zoom. Zoom access information will be published on our website.
Visitors or Guests are welcome.

Because of COVID-19, we recommend observing current masking and social-distancing guidelines as much as possible. Consider attending by Zoom if you or others in your family are in a high risk category.

Genealogy SIG: **No meeting** (3rd Saturday).

HELP CLINICS

December 4, 9am - noon at John Ruehle center
December 15, 9am - noon at John Ruehle center
Members may request Remote Help on our website at https://bvcomputerclub.org at menu path Member Benefits ►Remote Help .

MEMBERSHIP

Single membership is $25; $10 for each additional family member in the same household.
Join on our website at https://bvcomputercub.org at menu path Get Involved ►Join/Renew, by mailing an application (from the web site) with check, or complete an application and pay in person at any meeting.

CLASSES

(At BVCC Training Center)

Tuesday, December 7, 9am -11am. "Data: Where Is It and What To Do With It", with Pete Opland.

Tuesday, December 14, 9am – 10:30am. "Installing WiFi Printers", with Pete Opland.

Advance sign up required for each listed class (**Maximum attendance 8**): For reservations: email to edu@bvcomputerclub.org, or sign up at the General Meeting. Classes are **free to Computer Club members.** Class access information will be emailed to those signed up for the class the day before class.

Check the monthly calendar and announcements for any last minute schedule changes at https://bvcomputerclub.org .

NEW OR RETURNING BVCC MEMBERS

We are pleased to welcome the following new members or members returning to BVCC after an absence since last month's newsletter:

Nancy Bendickson Gary Magelssen Fran Hamilton

WHAT IF I NEED TO BACK OUT A WINDOWS 11 UPGRADE?

By Joel Ewing, President Bella Vista Computer Club
president (at) bvcomputerclub.org
Bits & Bytes, December 2021

The PC Health Check tool has been fixed to more-accurately assess whether a computer running Windows 10 can support Windows 11. If you are running Windows 10 on a hardware platform that will fully support Windows 11, you may have received, or may soon receive, an option to upgrade your system to Windows 11. This is not a decision you are forced to make quickly, as Windows 10 will continue to be supported until October 2025. In any event, you should always insure you have adequate backups before embarking on any major software upgrade.

See the "Windows 11" article in the September Bits & Bytes for additional information. If you have some older peripheral devices (printer, scanner, etc.), it is possible these devices might be supported initially, but not be supported on Windows 11 at some point in the future, should the vendor fail to update the device drivers for that model to the new Windows 11 standards by the time those standards start to be enforced. It sounds like there is a possibility that many months after an upgrade to Windows 11 you could find yourself with a choice of either replacing a peripheral device with a newer model, or if several years of Windows 10 support remain, you might want the option to roll back to Windows 10 and defer purchasing a new device for a while.

An article at zdnet.com ("You can easily roll back Windows 11 to Windows 10, until this bonkers policy kicks in") points out that if you upgrade Windows 10 to Windows 11, the Recovery Option of "Go Back" to Windows 10 is only available for a very limited time – namely, just for 10 days! Obviously the longer you have successfully been on Windows 11, the less likely you would decide to fall back to Windows 10; but for some, 10 days may not be long enough to verify that all the depended-on application and device features are fully functional.

Should you find performance issues or compatibility issues with some of your peripheral devices after that, a simple return to Windows 10 with "Go Back" is no longer an option.

To cover yourself for the possibility of a roll back to Windows 10 after more than 10 days have elapsed, it is essential before doing an upgrade to Windows 11 that you first make a full-image (not just user data) backup of your hard drive using some utility like the free version of Macrium Reflect, and be sure you have access to the corresponding stand-alone recovery media, just in case.

Without a recent full-image backup, the only way to return to a functional Windows 10 system beyond the 10-day "Go Back" period may involve a re-install of Windows 10 and all added applications, and many hours of work.

BROWSER HTTPS-ONLY MODE

By Joel Ewing, President Bella Vista Computer Club
president (at) bvcomputerclub.org
Bits & Bytes, December 2021

The Problem

A web browser like Firefox, Chrome, or Edge can communicate with a web site using the standard, default insecure HTTP method, or you may use a URL that starts with an explicit "https://" to indicate that secure encrypted HTTPS access should be used. In order for this to work, the website in question must be configured to support HTTPS. Part of that support requires the website to own a security certificate issued by a trusted third-party that in effect certifies that the owner of the certificate is indeed the organization that "owns" the domain name. The process of issuing those certificates requires that you own/control the domain name, so getting a certificate for a domain you do not own would be very difficult.

HTTPS encrypted communication with a website insures that no party on the Internet between your computer and the website that sees you data packets would be able to read the data. In addition, your web browser uses the security certificate at the website to verify that the party at the other end of your communication is indeed the party that owns the intended domain name, and not someone who has intercepted or somehow managed to mis-direct your communications and pretend to be the intended website.

There have been efforts in recent years to get all websites to support accessing all web pages via HTTPS, even if they don't deal with information normally deemed sensitive. Many websites that do support HTTPS are now also designed to automatically redirect a web browser that attempts to access the website with default HTTP protocol to instead switch to HTTPS. When this occurs, the browser will give some indication, like a "lock" icon" next to the address field and "https://" in front of the address, to indicate that your communications with the website is now secure; and if the security certificate is not "correct" for the domain name of the website, you will be alerted by a security warning that the party at the other end may not be the domain name intended.

The one hole in this verification scheme it that if you start with the default HTTP access, some third party could intercept that unencrypted access with no security warning, and then re-direct your communications to HTTPS access at a slightly mis-named bogus phishing website with a matching security certificate. You would see the normal indications of a secure connection being established, and if you didn't notice that the URL address was different than usual, you could be fooled into trusting the phishing website.

The odds of such an occurrence are pretty low, but not impossible. It would require corrupting in a very specific ways either a router somewhere between your computer and the target website or a domain name server (DNS) that you are either directly or indirectly using. You or your target website would have to be a high-value target to be worth the effort.

A Partial Solution

Firstly, it must be said that for the average computer user, the risk mentioned above is pretty small compared with the risk of reaching a phishing website by other means. The most common way to encountering a phishing website is by trusting a link in an unsolicited email or a link on an unfamiliar website. Using HTTPS provides no protection from fraudulent websites if you trust links from untrustworthy sources.

But, assuming you are already observing safe computing practices, to pose yet an additional obstacle to a phishing attack it would be best that your first access to a website is via HTTPS, rather than allowing an unverified website to handle the redirection to an HTTPS URL

The simplest approach is a manual one: All websites that handle financial transactions or have any kind of login must already support HTTPS access. Change all your browser bookmarks/favorites saved websites and add "https://" (unless it is already there) in front of the address for all financial sites and retail sites that have login information that is sensitive because of associated credit cards. If you use your browser for webmail access for email accounts that can be used to reset passwords at other websites, those webmail sites should also be considered sensitive.

For new websites that require logins, be sensitive to whether the way you save the website URL for future use includes a preceding "https://" and adjust it if it does not.

Another approach is available in the current versions of the Firefox, Edge, and Chrome browsers, which include a relatively new (as of 2020) feature called HTTPS-Only Mode that forces the default HTTP access to be upgraded to HTTPS by default. You might want to give this a try, as it can eliminate the need to check and manually change saved website URLs to include "https://". If you find a website for which this causes problems, you can either temporarily turn the feature off or add that website as an "exception". I've been experimenting with this feature in Firefox.

The one Internet website I've seen have problems so far with HTTPS-Only enabled is huffingtonpost.com or huffpost.com: some of their videos don't seem to work in that mode. Adding those site domains to the "exceptions" allowed the videos to function. Perhaps forcing a video stream to be encrypted may have been disallowed to reduce the overhead of encrypting the large number of bytes in a video stream – or maybe it's just a configuration issue. Making a problem website an exception for browser auto-HTTP-to-HTTPS upgrade does not prevent the website from doing its own re-direct to HTTPS.

You will also find that web-server interfaces used to manage devices on your Local Network may also lack support for HTTPS. These devices are only designed to be managed locally, not across the Internet. This may include WiFi routers (mine for example), home automation controllers, etc. As long as these servers are not made directly reachable from the Internet and your WiFi network is secured by an encryption password, accessing these device with HTTP is not a security exposure.

Firefox

To enable HTTPS-Only Mode in Firefox go to "Settings", "Privacy & Security" and scroll to the bottom to find "HTTPS-Only Mode". You can enable it just for "private windows" (opened from a Firefox menu option) or for "all windows". When enabled for "private windows" only, if the website fails in a private window, you can

always choose to run using a standard browser window. The ability to add "exception" domains is only available with the "all windows" option.

If an attempt is made to default to opening a web page using HTTP and upgrading that request to HTTPS fails, you will receive a warning "HTTPS-Only Mode Alert, Secure Site Not Available" and you are given the option to continue with just HTTP or Cancel. If the HTTPS failure is caused by an incorrect security certificate, you do not get any option at this point to review and override the certificate If there is only some internal piece of the web page that is dependent on HTTP, it is possible part of the page may fail to function without providing any specific error message.

I have occasionally run into links that will get the "Secure Site Not Available" warning. Sometimes when you allow it to continue and the website is reached, it is able to switch to HTTPS secure mode. Not sure what is going on to cause that, but possibly some configuration issue on their end. After running in HTTPS-Only mode for about a week, I haven't found many sites with other issues with HTTPS-Only mode; although it has meant when I find a website that does have a problem, my first response is still to retry with HTTPS-Only disabled to prove that isn't the cause. At this point I am continuing to run with HTTPS-Only mode, as it helps to make you more aware of the few websites that do not support HTTPS secure communications.

Chrome

Under "Settings", "Privacy and security", "Security", scroll to the bottom for "Advanced" and enable the option to Always use secure connections". If you go to a website that support HTTPS correctly, you will see a lock icon that shows HTTPS is being used; although it does not show the actual "https://" in the address field until you select the address field twice.

Going to a website that that supports HTTPS but has problems with its security certificate results in a window with "The connection to … is not secure" with an option to "Continue to site" or "Go Back". It is not clear what "Continue…" means in this context, but I think it means accept the questionable certificate as valid and proceed using HTTPS.

If you go to a website that does not support HTTPS at all, you get the same message, but in this case "Continue" will continue, using HTTP only.

It would be better to provide more information about the nature of the problem to make a reasoned decision about whether it is safe to Continue or not, and what the consequences might be.

Edge

Edge uses the same underlying engine as Chrome, but at this point the "always use secure connections" option by default is well hidden. Without a Google search you would never know it exists. To un-hide the option you must change one of the internal flags for edge by placing the following value in the Edge address field:

edge://flags/#edge-automatic-https

and then change the status for that Edge flag from "Default" to "Enabled" and then restart Edge.

After restarting Edge, you will finally see under the Edge "Settings", under the Settings menu "Privacy, search, and services", and then in that under "Security" a new option to "Automatically switch to more secure connections with Automatic HTTPS" which when Enabled, will initially be "only on websites likely [not explained] to support

HTTPS". You can choose to change the option to "Always switch from HTTP to HTTPS", which sounds like it should work similarly to the Firefox "HTTPS-Only" on "all windows" mode. Although there may be some subtle differences.

If the website can't support HTTPS, Edge at least gives some reason for the failure along with "Your connection isn't private" as an explanation for the failure. That explanation may or may not be helpful.