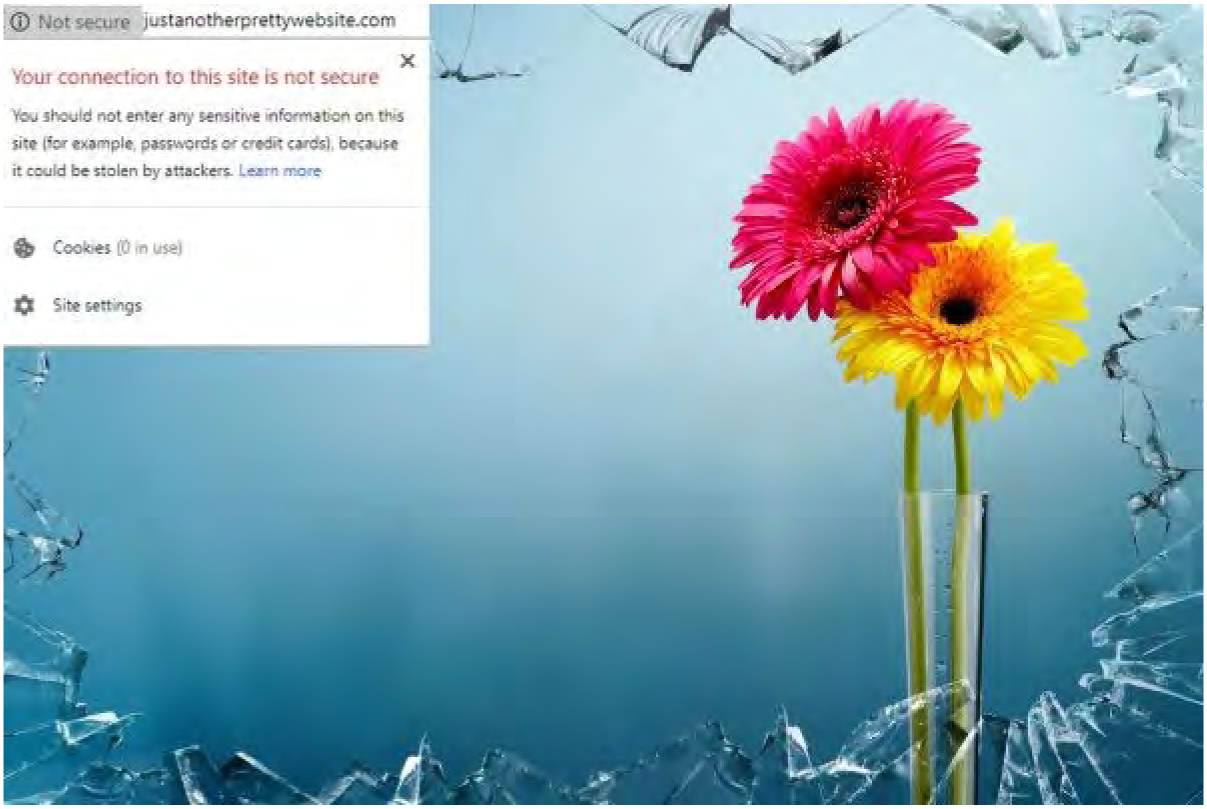
Science Translations
Established 1990
PC410.COM™

Managed Services,
PC Consulting, Sales, & Service in Central Maryland

# Not Secure?



ⓘ Not secure justanotherprettywebsite.com

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

Starting in July, Google Chrome will start warning that every unencrypted website is 'not secure.' That's the browser software, not the search engine. Google, the search engine, has given higher-on-the-page benefits to encrypted 'httpS' web pages for a few years now. This is a step up; both Chrome and Firefox have been warning about unencrypted webpages that include forms or passwords, but this Summer, the warnings about unsafe sites will show up everywhere on Chrome. As a web user, this matters when you visit web pages; as a business owner, it's very important that your web site has an https address.

## Back to Basics: https

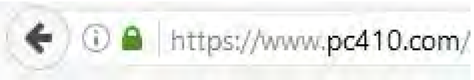
First, http means "hyper text transfer protocol." https adds an 's' for 'secure.' Not safe, that's not the same as 'secure.' Hyper text is a page that has something you can click on to do things, usually go to other pages or play a video or use a script to help fill in a form. 'Transfer protocol' is just a standard way to send these pages over the Internet. 'Secure' means that the pages are encrypted while they're moving over the web, so that no one else can read them or mess with them, or add anything like a dangerous script to them. Bad sites can also be encrypted, so malware can be on an encrypted https site; that does not make it safe. So 'secure' means locked by the original site, but not necessarily 'safe'. A locked door with a key under the mat is also secure, but not safe.

The encryption that makes all this happen is based on something called an 'encryption certificate,' which at its mathematical basis, is a pair of very, very large prime numbers that are used to encrypt the web page at one end of its voyage through the 'net, and decrypt it at the other end. The certificate is issued by a 'certificate authority' company, and there are a few hundred of them, and there is a process for revoking the keys if they're mis-used.

There's also a process when you visit a site, called a 'handshake', where the server and your browser decide what those keys will be, and exchange them without revealing them to any party that can see what they're sending back and forth. It used to be that the handshake and the encryption were expensive, both in computer time and for the cost of buying the certificate. That's no longer true; computers and the internet are far faster than they were when secure pages began to show up in the 1990's.

## Certificates

There are also several types of certificates. The least expensive is called 'domain validation,' and it encrypts web pages and email, and guarantees that pages using that certificate can only come from one domain, like "mydomain.com". These certificates are good enough for most small businesses, and good enough to avoid that 'NOT SECURE' message. Domain validation certificates used to cost around $100 a year. Now, they're free from Let's Encrypt or AutoSSL, and they're actually better than the paid certificates–they auto-renew.These sites show a small padlock.



https://www.pc410.com/

Beyond domain validation, there are also 'wild card certificates', used so that multiple web sites on one domain can share a certificate, like 'www.mydomain.net' and 'orderform.mydomain.net', and then there are 'extended validation' certificates. While a domain-validation certificate proves that the page is on your domain and no other, an extended-validation certificate proves the identity of the company running the site, and not just the location. Extended-validation sites are usually shown in browsers with a big green padlock; look for them on banking sites.

## Action Point: Web Browsing

As a user of the web, when you see that 'NOT SECURE' message, will you care? You should care if it's a bank, or if it's a web site where there is a login form that could be seen while passing through the internet. Even if it's just a page with no login that you're just surfing across, the 'NOT SECURE' message means that the site could have injected content on it.

What's 'injected content'? Well, that's code added to a page, sometimes extra advertising, or malware, especially if you're using the web on open WiFi, or worse, outside the USA at an internet café. Or locally, Comcast can (and does) inject code into web pages to pop up sales pitches for upgrading modems. Other internet providers are doing the same with tracking cookies, in order to make more money off their paying customers. Encryption breaks all of that. The point: https pages are secure, and in most cases, safer. Don't trust the 'NOT SECURE' pages.

## Action Point: Web Hosting

Do you have a company web site? Does it have an encryption certificate, so that it won't be flagged as 'NOT SECURE' in July? Or right NOW, if there's a form of some kind on the page? It's time to encrypt every web site. Even simple little one-page 'business card' sites should have encryption; it gets higher rankings on Google web searches, and it's much easier to set up email on smartphones if the domain has even the basic 'domain validation' certificate. Do you use an iPhone? Recent software changes on iPhones and iPads fight setting up unencrypted email, and break unexpectedly. Any encryption certificate makes iPhone mail easier to set up and more reliable.

If your web site is not yet secure, call me. Converting web sites varies in cost with the complexity of the site; some simple sites, already hosted here, will be converted for free, and some will be a larger project. In both cases, plan to have all your web sites https and secure by July. And the encryption certificates are free.

# Windows 10, Version 1803 is 'The April Update'

Welcome to the April update

This Windows 10 update contains a lot of new features. Start here.

1
Resume past activities in timeline
SEE HOW >
2
Share files with nearby devices
LEARN HOW >
3
See what else is new
LEARN MORE >

The lastest semi-annual "feature update' for Windows 10 is available for manual install now, and will start to install automatically soon, probably starting in June. Again, this is one of the big feature updates that take from 40 minutes to 2 hours to install, longer if your internet is slow. At this point, I've installed it on some spare computers without problems. It's late; this was supposed to be the 1803 (March 2018) update, and it just became available on the last day of April. So it's early days, and and whatever problems it causes aren't well-known yet. At this point, most users should not choose the early installation. As usual, the update is not optional; it will force installation within a few months. Best to wait a month, and then scedule that update to install overnight.

**What is New in the April Update?**

Homegroups are gone, so if you're one of the 6 people who chose that alternate way of building a network, you will have to switch back to using good old reliable workgroups.

Timeline is new; it's built-in file versioning that will let you move back in time to how your computer and files were at some date in the back, usually up to 30 days. More on that once we've worked with the final version of it.

As always, if you are using an industry-specific program that holds all your data, ask them if they're ready for Windows 10 version 1803 before you upgrade.

Reminder: Run 'winver' from the start menu to see the Windows version that your're running. Nearly all Win 10 machines are at the '1709' or October 2017 update right now, also called the 'Creators Update.'

**Contact**

Address all editorial and unsubscribe requests to:
Jerry Stern, Editor, Science Translations, P.O. Box 1735, Westminster MD 21158

Phone (410) 871-2877