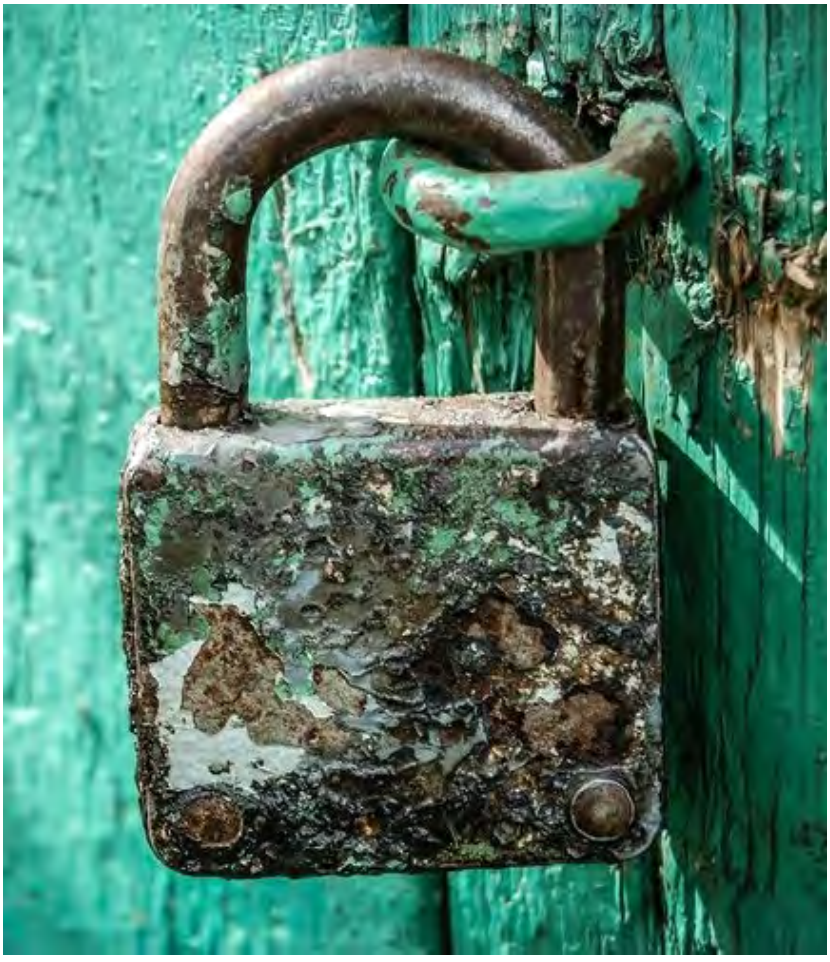
Science Translations
Established 1990
PC410.COM™

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

Coming This Summer: PCI Compliance and 'Not Secure' Web Site Warnings

Some of you have begun to receive notices about PCI Compliance. While that's not new if you have a credit card terminal, PCI Compliance is starting to show up for logins on secure web sites as well, especially sites that handle credit cards, medical information subject to HIPAA regulations, or financial information under FINRA control, and a few other areas.



PCI Compliance is, basically, “a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure

environment." Translation: If you accept credit cards in a gadget than connects to the internet or on a web page, you have standards to match. If you are a consumer using credit cards on the internet, there are encryption issues to watch out for.

If you have a credit card terminal, PCI Compliance includes, generally twice a year, both a security survey and a remote scan of your IP address to make sure that the terminal's connection cannot be accessed by some other device. A security camera DVR (video recorder) is the usual issue. Call me before adding a security DVR if you already have a credit card terminal, or vice versa; there are ways to isolate those devices so that they cannot affect each other.

What is happening this year is that there is an expiration coming up at the end of June 2018 for TLS 1.0. That's 'Transport Layer Security version 1.0', which real security experts have encouraged turning off for years now, and replaced with version 1.2, but which the PCI Council, an industry group in the credit card industry, has delayed removal of to this year.

So what is TLS? Transport Layer Security is the new name for SSL, or Secure Sockets Layer, and both of these are encryption methods for sending information between your computer and web pages. TLS replaced SSL, so SSL is an old name still in use in some software. TLS includes both the encryption of data, and a method for a computer and a web site that have never connected before to exchange encryption keys through an open internet connection, while not allowing any system observing that process, to be able to read those keys. That's complex, but it all happens in around a second every time that you connect to any encrypted (http**s)** web page.

The very-official announcements you may receive about PCI Compliance in the these coming months will boil down to this: Use the new versions of TLS, either version 1.1 or 1.2. That's a setting in the Control Panel of Windows 7 and higher, easy to do. It's under Internet properties, Advanced, Security, uncheck SSL 3 and TLS 1.0, add checks to 1.1 and 1.2 if not already there. (Or call for assistance.)

Windows Compliance

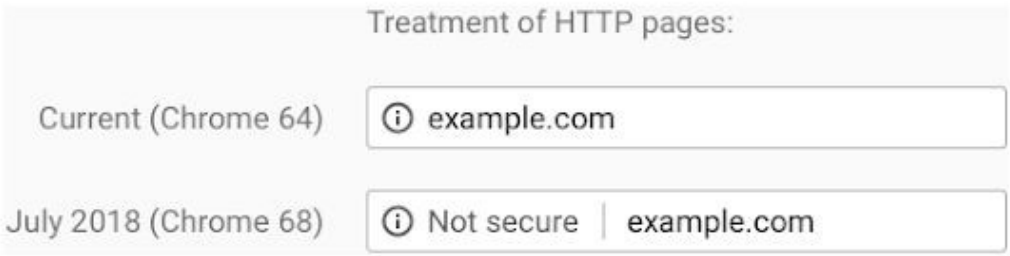
Running Windows XP? Don't use it for banking of any kind. Even with the best antivirus software, XP cannot support these new encryption methods, and can not be made to be PCI Compliant. Most banking sites won't even allow a log-in with Windows XP, and if they do, change banks NOW.

There's another important part of PCI Compliance: The software used in a PCI Compliant system must be able to receive security patches. Patching for Windows XP ended in April 2014. Windows Vista ended patching in April of 2017. Patching for Windows 7 will end in January 2020, so starting early in 2020, Windows 7 will not be accepted for working with credit cards, financial information, and medical information subject to HIPAA, FINRA, or SOX (Sarbanes-Oxley) regulations.

Bottom line: In Windows 10, there is a setting change, not much else for most users. For older Windows, plan on replacement or no more banking, medical, or financial use after 2019.

Warnings On-Screen

Starting around July 2018, Chrome software will start treating all non-encrypted web sites as 'not secure'. Here's what that will look like:



What does that mean for web surfing? Well, if the site where you see 'Not secure' is somewhere you can visit without logging in, not much. If it's a bank or any site that accepts credit cards, it's unsafe in some way, and it's usually not worth trying to to find out the details

of “Is it good enough to trust?”, as any site that can't set up a basic encrypted web site should not be given your credit card information.

That 'not secure' will also apply to sites with an encryption certificate, but which have been designed to use un-encrypted content on the site. That's called 'mixed content' or 'insecure media'. Usually, that means that a logo or a photo or an advertisement has been added that isn't being encrypted. Without reading the page code in detail, there's no quick way to know if 'Not secure' means something minor like an unencrypted logo, or major, like an unencrypted form submission.

If you have a web site, there are tools to check if your site will become 'Not secure' this Summer. Look for Google's “Chrome Canary”. That's basically a test product, that looks like what Chrome will evolve into a few months from now. Like any test or 'beta' product, it's not for all users, and will crash in odd ways. Using it for testing is OK, but it should not replace your current-model browser.

Spring Creators Update Starts Arriving in April

Microsoft is continuing their semi-annual schedule for feature updates to Windows 10. This is another free update, non-optional, that will change how Windows works. New features are only partially announced so far, but will include the ability to mute a single tab in Edge (already available in all major browsers). Bluetooth file transfer is new, but Bluetooth is mostly used on phones, not Windows, so far.There's a Timeline, which will show your history of programs and documents, on "all" your devices. Most likely, that will be limited to devices that use your Microsoft account for sign-in.

Timeline, as described so far, is impossible to do that without sending a lot of information to Microsoft servers; we'll have to watch that for the security and privacy implications. As always, I continue to recommend 'local' accounts on nearly all Windows 10 systems, with exceptions only for a few mobile users who need file syncing between multiple systems.

Newsletter Subscriptions

Business Owners: If your entire staff should receive this newsletter, let me now, or just send a list of individuals who should be added.

Contact

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

Phone (410) 871-2877