Stuff that just makes you want to scream! – by D'Rock

Over the past month or so, there have been two highly publicized computer bugs that have sent many into a frenzy. Usually when this happens, we field lots of the same questions that many our customers have and try to calm their fears. At this point, you have probably heard of the issues with Internet Explorer that got Homeland Security concerned and Heartbleed, the security glitch that affected a good portion of the World Wide Web. As of today, both of these issues have been resolved, but you still may want to take precaution from their aftermath and future issues.

The dust has finally settled that was kicked up by the Heartbleed bug that affected internet giants, such as, Google and Yahoo!. The problem itself affected web servers that use OpenSSL for their TSL (Transport Security Layer). Most people could care less about how the problem occurs, or even what causes it. They just want to know how it pertains to them and how to protect themselves from it. In this case, the main thing individuals need to do is; change their passwords. If there is a website that you log in to using a user name and password, you are potentially at risk. Best thing to do is change your passwords to any website that contains sensitive and/or personal information. Big ones would be email, financial, or anything you store credit card information for shopping. Once changed, make sure you keep your new information. A recently changed password is much harder to remember than one you have used for 3 years. Even if the website was not at risk, it never hurts to change your passwords every so often. The other thing to consider is that this bug attacked outside servers that contain your information. Having antivirus software on your computer **does not** protect you from this type of breach.

Another issue that has made major headlines was a glitch in Internet Explorer that had Homeland Security discouraging people from using Internet Explorer all together. This problem also has been patched by Microsoft and I would encourage you to go ahead and run your Windows updates. Even those of you still using XP, Microsoft has pushed out the update, even though it is the post XP support era. This is most likely the last update XP will ever get, so consider this your get out of jail free card. The problem itself could potentially allow a hacker in a remote location to take control of your PC. This could happen if you clicked on a wrong link or had a prior infection that redirected you from your requested destination. Many people use Internet Explorer and do not even realize it. If you have a Windows PC, you have Internet Explorer on your computer. Knowing this information, hackers often make Internet Explorer the target of their attacks. Considering this, it still may be a good idea to begin using Mozilla Firefox or Google Chrome. Do not worry if you are afraid of learning something new. These browsers work very similar to Internet Explorer. You will probably even find liking these browsers much better. As a computer tech, I recommend making this switch. You can use these on PC or Mac, and I prefer both of these browsers over Internet Explorer. So, run you Antivirus scans, download new Windows updates, and begin to learn how to use Firefox or Chrome. Keeping up with these three things can protect you now *and* in the future.

Something new just this week is an email that comes disguised as a "Fax Message". In todays world we get emails on our phones and texts in our emails, why wouldn't we get a fax in our email? Looks real, if you google the company that the fax/email was from, it is a legit faxing company. So how do you know if you should open it or not? This is where your red flag antenna needs to go up, ask yourself, should somebody REALLY be sending me a fax or any other email that looks suspicious? If in doubt, double check the email, looking for misspellings or other grammatical errors. Look at the attachment, it asks you to open…if it doesn't have identifying marks, like company name or document names you recognize, DUMP IT. Nine times out of ten, if someone sends you something important enough to open, they will notify you or you will be expecting it.

Unfortunately, the high tech world we live in almost forces us to function on the grid and the internet. Criminals like taking the easy route and many of them find the internet the easiest medium. So we are forced to find ways to protect ourselves as well as we can. There are good guys out there, but the rat is usually a little ahead of the cat. So take precaution and be aware of your surroundings out there.

One final note…. We are continuing to see good folks scammed by phone callers who say they are with "Microsoft" "Nortons" "Windows" etc….. PLEASE NEVER let anyone who calls you on your computer and do NOT pay them any money to remove an infection! We can say with 100% accuracy that none of these companies will call you to help you "clean up" your computer! Be aware!! Call us for help before you make a costly mistake!

Blog by David Rockwell…..you can contact him at 704-482-0057 or david@painlesspc.net
Computer Connections, Inc. 6-5-2014