TECHNOLOGY TODAY

Friendly Connections IT
STAY CONNECTED

Insider Tips To Make Your Business Run Faster, Easier, And More Profitably

August 2016

Inside This Issue…

Windows 10 Security Special

There are a lot of security concerns with Windows 10 and anyone using the system should be aware of it. Microsoft collects a lot of data to provide services such as Cortana and the default Win 10 settings share even more with your 'friends'. We have a recommended security standards baseline for both residential and business users.

For $45 in shop or $60 remote we will reset Windows 10 security settings to ensure it is as secure as it should be. Call us 512-931-4134.

The first anniversary of our second 10 years

A year ago we were hard at work preparing to end our franchise contract and create the company we have now become. At the time we were moving away from the franchise model of "Break/Fix" on site service. Part of the reason for that was to keep from direct competition with them. One of those legal things.

That is all over now and we are free in every way from the corporation that owns the franchise. Our preferred mode of operation continues to be joining in partnership with our clients so that we can be more proactive. This allows us to continuously monitor the systems, to ensure critical updates of Windows and other programs are expeditiously installed, to clean up minor problems before they become major ones, and to manage backups for emergencies. Our list of partners in such agreements continues to grow as nearly all of them quickly see the benefit. Our longest standing Friendly Residential Service partner brought his PC in a couple of times a year with malware on it. We put him on the program and he has not come in since, not a single issue. He takes advantage of the program by calling in occasionally to ask about whether he should respond to an email or some other question. We're always happy to help.

We recently reviewed one of our partner businesses that showed similar results. Before and after differences in performance and efficiency are easy for us to demonstrate.

That said we are also happy to go on site, happy to fix that broken laptop screen brought into our shop and happy to set up networking (or secure it) in a home. Our services range from the simple fix to the long term relationship that best benefits our partners.

And now comes with 11 years of experience!

Bill Schubert

More bad ransomeware news

So you are the perfect PC user. You NEVER click on web links in emails. You ALWAYS keep your Windows, Java and Flash updated. You KNOW your antivirus is working.

Next thing you know all of your documents are encrypted as is everything in your Dropbox (OneDrive, etc). How did this happen when you are so careful?

Here's the problem. There are applications crawling around the internet looking for security holes in web sites. Graham Cluley presents a long version of what I'm going to relay in this newsletter. Go here [1] if you want to read the entire article and its links. Mr Cluley is one of my go to security people.

Here's the gist of what is happening. Web sites are built on software that typically has a lot of 'plugins'. The plugins and the site itself are set up to interact with people accessing them. Click on one thing and you get a contact form Click on another and you download something. Anytime there is user interaction there is potential for someone who writes malware to 'infect' the link. There are software writers who write 'bots' which are pieces of software that crawl around the internet checking site after site 24 x 7 trying to find that crack in the software that will allow them to insert a simple piece of code. That code redirects an unsuspecting user to a different web site which automatically downloads a virus. That virus has a ransomeware payload and suddenly all of your documents and pictures are encrypted.

Years ago I actually saw this demonstrated on the Better Business Bureau site. It was only there for a short period of time before they caught it but the video showed the user running a search for BBB. It actually found the right site, Better Business Bureau, but in the background and unknown to the user the site briefly redirected the computer to another site which downloaded a virus in the background.

"But I have Antivirus!!" Well, yes. And that antivirus has probably protected you from a hundred virus attacks. Unfortunately this one was only created last week or yesterday or today and the antivirus doesn't know about it yet (called a Zero Day virus).

I would venture to say that nearly every computer will some day be infected. No matter how good you are, how careful you may be, no matter how vigilant it can happen. And if your PC is infected you must be prepared to have all of your data compromised. I'm sorry but that is the truth.

What to do? Well, all of the usual things. Another one of my security gurus, Brian Krebs, summed up his thoughts here [2]. They are:

1—If you didn't go looking for it, don't install it.

2—If you installed it, update it.

3—If you no longer need it, remove it.

I'm a fan of Acronis. My PC set up is fairly complex. It took me weeks to get it just the way I want it and I've already forgotten much of what I had to do to get it here. So I create a full image once a week and update it daily. If I am the victim of a virus attach (or just a dead hard drive) I have only to restore the image and everything returns as it is right now.

But more importantly is backups. If you've ever read any of my articles you know that backups are the final wall between you and the barbarians at the gate. I really would laugh at a ransomeware attack. Really. My reaction would be to restore my PC with Acronis and restore all of my files using the backups that we run every night.

If you care about it, back it up.

If it took you time and energy or money, back it up.

If it is that one picture of your child that you most cherish and the only copy is on your laptop… well, you can guess… Read the next article.

FC Friendly Connections IT
STAY CONNECTED

The Backup Basics

How to design a backup strategy

Your business continuously generates additional data. Being without your data for even an hour could be expensive and extremely detrimental. The answer is to back up everything. All the time. First, you need to choose what you'll use for backup, and then you need to decide on a combination. One source of backup is never enough. Here are the readily available options.

Direct attached storage (DAS)

DAS devices connect to your PC or server (usually via USB). They are handy and portable, which means they could be taken out of action at the same time as your main storage if the issue is something like theft or fire damage. That makes them a great first line of defense, but don't make the mistake of depending on these devices for your entire archiving and disaster recovery plan.

Network attached storage (NAS)

NAS appliances connect directly to the network. They have file server and redundancy capabilities, and in some cases, they have the ability to synchronize data with a compatible remote NAS. Like USB they are IN the building and therefore susceptible to building hazards.

Private cloud

This is buying a server located in a data center. You own the equipment and the data in it and the data center manages the security and environment. This is an excellent, if somewhat expensive, solution. The data center can be located far away from your current building.

Managed Cloud

This is what we use. We have proprietary software that backs up computers to the Amazon Cloud (the same one Netflix and many other major corporations use). Since the data is encrypted before it leaves the building it is secure and Amazon's availability is as near perfect as can be achieved. Their storage facilities are as secure and safe as possible and the price is reasonable.

Our customers depend on Friendly Connections FC backup services which are set up and monitored by our purple gang. We all get a daily message with the status of our backups and a ticket is automatically created in our system if a problem has developed.

The right combination

A good starting point is the rule of three: 2 + 1.

2: A full copy of everything on at least two different physical devices (DAS or NAS and the originating computer)

PLUS

1: A third copy that's offline at another location

The offline version is critical. It can't be hacked, it can't be corrupted accidentally, and it's harder for someone with malicious intent to access (a rampaging ex-employee, for instance). Like everything else associated with data, a good backup strategy involves simple math.

Let us make your data bulletproof so you can sleep better at night.

Quotes

Ah, summer, what power you have to make us suffer and like it.
Russel Baker

A perfect summer day is when the sun is shining, the breeze is blowing, the birds are singing, and the lawn mower is broken.
James Dent

The pleasure of jogging and running is rather like that of wearing a fur coat in Texas in August: the true joy comes in being able to take the damn thing off.
Joseph Epstein

It's a cruel season that makes you get ready for bed while it's light out.
Bill Watterson

Happy birthday to all the Leo's out there. **We deserve it!!**

"Are they real or is this a screen saver?"

Roboform and other lifesavers

I've got something over 200 passwords now and here is what my average password looks like:

2d9#Tog#$8

Do I remember it? Nope. I've got software to do that. Otherwise all of my passwords would be named after my dog and her name is only three letters long (Zoe, in case you stop by the shop). Read quietly I think she's asleep.

I only have to remember one password. It is the password to my Roboform. This program is not the only choice, just the one I started with and haven't moved on from. My sister did the same and ended up with Last Pass which she likes.

Here [3] is more information from a post I wrote last year.

These programs can take a little effort up front but the security is worth it. No more slips of paper, no more password recovery, no more having your banking password be **zoe1234**.

Ok that last one was never true. But it could have been.

Links from the newsletter

1. http://s.fcofg.com/soaksoak
2. http://s.fcofg.com/rules
3. http://www.fcofg.com/passwords/