Friendly Customers!
Friendly Connections!
Friendly Computers!

June 2014

Technology Today

"Insider Tips To

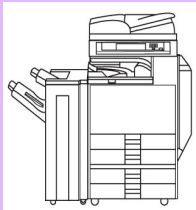
"As a business owner, I know you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

- Bill Schubert, Friendly Computers

Inside This Issue…

We have partnered with an excellent printing/copier/ sales and service company.

Copiers ASAP



Contact Todd Brevard at

512-948-9794 or 866-553-7262

for your business copier and printer needs.

Security Issue

When we first started Friendly Computers in 2005 malware appeared in the form of viruses on PC's that were destructive and occasionally went after passwords or data. But they were not very effective and not at all organized. The 'black hat' community—the murky behind the scenes groups that developed malware—were largely independent and only related with each other for the most part in a kind of competition for who was the best. The social engineering that occurred was to accomplish the task, to beat the system, to gain access but little more. A much smaller percentage of the general public were online shopping, banking, paying bills and living their financial lives on the Internet. And reading about malware and staying on top of the black hat people was exclusively in the realm of the IT professionals. It was a backwater. Interesting for the most part only to the geeks of the world.

In this year's first issue of my newsletter (available on the web at: http://s.fcofg.com/newsletter) I opened with the line:

2014 should be dubbed "The Year of IT Security", OR, conversely, a stolen title like "The Year of Living Dangerously" with apologies to Mel and Sigorney.

And it is turning out, six months into the year that I was onto something. From 2005 to the present the security of personal computers had moved from discussions among techies to the evening news. From being an annoyance to being a danger to society. From being in the realm of maladjusted petty criminals to being a marketable product of worldwide organized crime. From stealing a password and birth date out of a home computer to stealing 110 million credit card numbers from a major corporation.

But one thing that has not changed. **Nearly every story of the weekly criminal theft of data starts out with someone clicking on a link in an email**. That is what brought down Target (the first piece in a long chain of dominos). The security breaches that do not involve clicking on something usually involve not updating or not maintaining basic PC security.

So this issue is a collection of basic security definitions and thoughts on how to keep from becoming a target. Please call us if you have any questions about security. It is what we do every day.

Bill Schubert

Get More Free Tips, Tools, and Services At My Web Site: www.FCOFG.com

The 5 W's and an H of Malware

Understanding the problem is the first step in being able to defend against it. The following discussion of just what is malware was first published by me last year.

Who: Since the first PC, there have always been the kids flexing their initial programming skills by creating a virus. [Note: A virus is an application like any other but with the purpose of causing trouble of one kind or another] Then there are a lot of Asian entrants into the malware world as we hear about in the news (the Chinese Army among others) but the current success story, and this has been true for a while now, is eastern European organized crime. And I do mean organized. Think multi-billion dollar businesses working full time to separate you from a couple of hundred dollars and your credit card number (AND your mother's maiden name, date of birth, bank info, etc).

What: Malware is a generic term covering all forms of virus activity from the simple pop-up type virus advertisements and browser redirects to the killer 'ransomware' whereby one's data is encrypted and they must pay for the key. The tools are plentiful and freely available complete with malware 'Help Desk' support for anyone who wants to get into the business.

Where: The huge problem is that malware is ubiquitous. It is easy for me to say "Don't click on links if you don't KNOW what they are" but then the UPS email comes in and you are, in fact, expecting a package. Turns out that link is not specifically for your package but is the beginning of a malware attack on your PC. Or you can do everything right and still get caught by going to a web site that has been sloppy with their security and is infected thereby spreading the infection to you. Some major sites have been through this.

When: Well, the Internet malware café is always open. 24 x 7.

Why: This one is easy: MONEY!!! Billions of dollars. There are still kids writing malware but the really dangerous stuff is put together by very intelligent and motivated companies. And there are people who are paid upwards of $50,000 per month to create scams of social engineering like the UPS email just to get you to click on the link downloading someone else's virus. There is even software available that modifies existing malware just enough to basically create a new virus. Estimates of new malware start at something like 30,000 new virus signatures PER DAY to nearly 100,000. Mind boggling numbers keep the antivirus companies working full time to get the fix out as soon as they can to every new virus coming down the pike. Most antivirus programs now update every four hours for that reason.

And I'd like an H now, please, Pat.

How: Well, I've answered much of this question but it comes down to the fact that the Internet is available to everyone, or nearly so, now. And as with every other tool it can be used for the greater good and the greater bad in equal measures. The tools are out there and law enforcement is nearly always playing catch up. Some very interesting reading is available on www.dhs.gov (look for Cybersecurity in the Topics section) and under Scams and Safety on www.fbi.gov. A lot of good common sense advice.

Why Don't We Get Viruses?

Why don't we get malware on our PCs here at Friendly Computers? Fair question. Let's start with some honesty here. We actually did have a virus on one of our computers. It has been a number of years since this happened and the culprit will remain nameless (unless you know the name of my wife). And a couple of months ago I picked up some low level malware what we call 'pup' or Potentially Undesirable Programs. More about that later. But after nearly 9 years of being in business that is it. And considering that our entire team is online searching for parts or drivers, researching malware problems or new technology one might expect problems. I spend some time on social sites as any successful business does these days and our email address is available online all over the internet. Meanwhile in that timeframe we have conservatively taken in over 5000 computers with malware and fixed them.

So, what gives? Here's the list of what I think makes the difference in our shop:

1 - **We use AVG CloudCare on every computer.**

The CloudCare version is mostly for businesses but it allows us to keep watch for problems on our customer and our own PC's through an online console. Both the CloudCare version and the standalone version do as good a job as any system I've found and neither interferes with the programs we run. I've actually never seen AVG interfere with anything which is a major criteria in my selection of an antivirus system. One thing to keep in mind: No antivirus will defeat a user that is so determined to download something that they ignore the warnings. Read the fine print on EVERYTHING.

2 - **We update all of the PC's all of the time.**

No exception. Our server goes through a separate system of updating as should all servers. But the PC's, all of the recommended, automatic updates all the time. They are usually security oriented so there is never an exception to this (despite what many techs say, I've adhered to this for years).

3 - **We don't always browse but when we do we use the Chrome browser.**

This would start a war on the tech sites but I'm convinced that Chrome is the most secure browser. I've been using it since its inception and am used to it. Next choice would be Firefox but I never really liked the way it operates. Personal preference. A lot of this is personal preference but, hey, it has worked so far. The Chrome browser can be downloaded at www.Chrome.com.

3a – We disable Java on our Chrome browser.

If I go to a site that requires Java (and the sites will say that) I shift to Internet Explorer. Otherwise I don't want Java enabled since it continues to have a lot of security problems.

4 - **We have an excellent firewall on our network.**

This is a business class firewall. What that means is that I've got an appliance that sits between me and the Internet. Its primary job is to make sure that no one can get into my network who is not supposed to be here. Connecting to the internet is like connecting to a faucet and turning it on. Everything comes through and there are people out there who write programs that constantly look for unprotected connections. Having a good residential router performs a lower level of what we have and is generally enough protection. But a business like ours is more of a target and we have a better system. I am of the opinion that EVERY business should have a good firewall. They are not cheap but pay for themselves many times over with a single prevented incident of hacking. The firewall itself contains antivirus so it offers a second layer of protection in addition to preventing hackers who might want to do us harm.

The Lighter Side

"Computers in the future may weigh no more than 1.5 tons."
-- Popular Mechanics, forecasting the relentless march of science, 1949

"I think there is a world market for maybe five computers.
-- Thomas Watson, chairman of IBM, 1943

"I have traveled the length and breadth of this country and talked with the best people, and I can assure you that data processing is a fad that won't last out the year."
-- The editor in charge of business books for Prentice Hall, 1957

"There is no reason anyone would want a computer in their home."
-- Ken Olson, president, chairman/founder of Digital Equipment Corp.,1977

"So we went to Atari and said, 'Hey, we've got this amazing thing, even built with some of your parts, and what do you think about funding us? Or we'll give it to you. We just want to do it. Pay our salary, we'll come work for you.' And they said, 'No.' So then we went to Hewlett-Packard, and they said, 'Hey, we don't need you. You haven't got through college yet.'"
-- Apple Computer Inc. founder Steve Jobs on attempts to get Atari and HP interested in his and Steve Wozniak's personal computer

"To redeem your wishes, fill out all required fields, including username and password."

Telephones and the Computer

When I was growing up it was mail fraud. Pyramid get rich schemes through the mail. Then the computer came along and it seemed there were a large number of princes from African countries that were in a position to acquire money with a little help. I suppose that both of those 'opportunities' are still available but what I am seeing with my customers is more immediate now days. They get telephone calls from various people trying to 'help' them. It goes like this:

"Hi, I'm Mike and I work with Microsoft. We noted that your Operating System license is expiring and are calling to offer you a discounted renewal. If you will allow me to remotely access your computer I can apply the license and you will be set for the next three years."
OR
"Hi, I'm Mike and I work with McAfee. We are seeing a problem with your computer. It appears to have a virus on it and we need to get is taken care of immediately. If you allow me to remotely access your computer we can prevent you from having further problems."

I've even had a customer report to me that the person on the other end told her that if she did not cooperate not only this computer but any computer she owned in the future would be unusable. Fortunately she called us.

No reputable company, not Microsoft, not Google, not McAfee, not Norton nor any of the other many security services will ever call you directly. Ever.

If you should get such a call, just hang up on them. They are targeting a specific demographic just like any other marketer.

File a Complaint

This is all about collecting enough data to be effective. The person calling your house is likely part of a large organized crime group from an eastern European country. Currently that is where the billion dollar criminal industry is centered. It takes governments and large international companies working in concert to stop the crime. So reporting to a central database, no matter how small is your incident, adds to the pile of information and is critical to successful deterrence. Here are three of them:

www.ftccomplaintassistant.gov

www.stopfraud.gov/report.html

www.ic3.gov/default.aspx