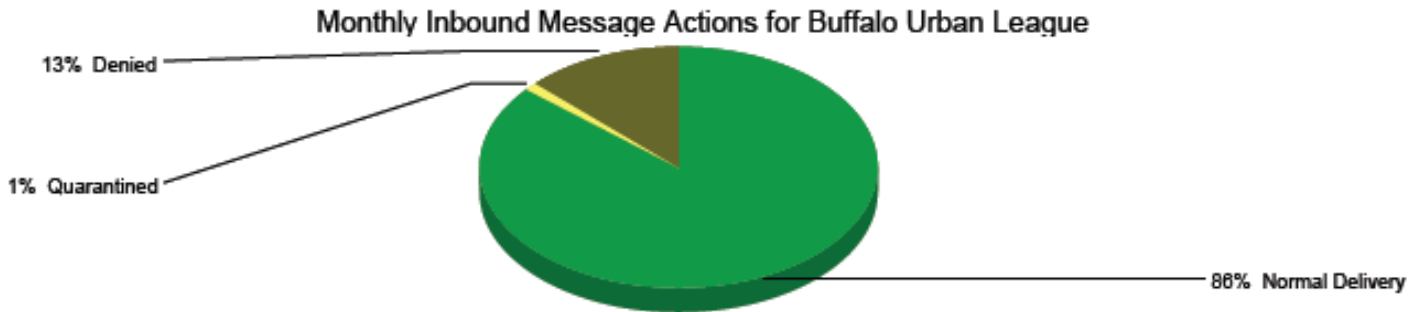


This may save your job and personally save you some serious money.



The above chart shows that 13% of last month's Buffalo Urban League inbound emails were stopped by our email antivirus program. That means that more than 1 in 10 things we receive **at work** are loaded with hidden programs that will prohibit us from doing our job on our computers. The good news is that our email virus protection is working. We pay to have all our email filtered through MX Logic (now owned by McAfee).

Now for the bad news. You go on the internet to sites not related to your job. Because of that, our servers picked up so many viruses that this week, our servers were so infected that many of us couldn't even log in. Things went so slow that those of you who could login couldn't get your work done.

The glaring fact is that the internet is now loaded with such aggressive spyware, malware and virus programs that just going to some sites subjects your computer to bad stuff that creeps into your account. There are "redirect" sites that look exactly like the usual trusted sites but will take you to some other page (that equally looks like it is where you belong). These web pages quietly install aggressively destructive programs that are timed and triggered to do their thing later when you're not aware. This is the reason your friends and relatives have their home computers so slowed down so as to be unworkable. This is the reason why our servers got so bogged down this week that we couldn't work.

Most everyone feels that (1) the Internet is some sort of rite of passage to the American Dream and prosperity and that (2) "someone else will take care of protecting us." This isn't reality. It isn't reality at home or at work. It's worse at work and here's why.

If your home computer gets screwed up, you lose everything on it because you have to have it reformatted. Then you have to reload all your software and if you've backed up your data, you get access to it again. After a couple of weeks and hundreds of dollars of cost out of your own pocket, you get to use your newly refurbished computer. That's bad luck.

If it happens at the Urban League, it's worse luck. The league loses thousands of dollars of lost work, shorting us in meeting our contracts. We, personally, lose more than hundreds of dollars if we lose our jobs.

Fact is, there is a war going on now and you and are in the midst of it. There are multi-million dollar groups oversees constantly launching aggressive software on the internet. They are based in countries where there isn't the technology or laws that care to go after them. All of it is extremely sophisticated,

articulately crafted to get you to click on something out of worry that you need protection or that there's something wrong with an account you have (that usually you don't even have). It's called "social engineering." It means that it is engineered to pray on your fears or your deepest longings.

How can we combat this when so much of our lives are on the internet? What can you do?

Simple. **At work, do nothing on the internet unless it is directly related to your Urban League job.** No shopping. No research for your kid's term paper. No music, videos, no wonderfully spiritually uplifting and heartwarming stories or pictures of dogs who have made it here to ultimately meet up with a soldier who befriended them while on foreign duty. Do not resend personal emails that you feel are personally meaningful. Do not send or receive emails from the person of your dreams, your spouse, your children who haven't talked to you in ten years. Even if someone sends you a story that changes your life, fixes your marriage or proves to be a pathway to nirvana, don't open it. Don't open, read or process personal emails at work. Please save that risky behavior for your home computer. Your friends and relatives might judge the Urban League as too restrictive in their computer use policies but at least we'll have a job that will support us in personal computer use at home or elsewhere.

I know this sounds boring and heavy-handed but we don't know how else to say this: **USE THE INTERNET ONLY FOR WORK THAT IS DIRECTLY RELATED TO YOUR JOB. That's the only way we can stem the expensive leak of downtime from virus infections here. Each of us need to focus on this task if we where we work is going to economically survive.**

At home, here are some initial words of advice (because it is your money that is at stake).

1. Be sure you have a router installed between your cable modem internet connection and your computer. [Internet – Cable Modem – ROUTER – Your Computer]
2. Buy Norton (Symantec) *Internet Security Suite* and install it on every computer in your house. The internet is so bad and invasive, now, that you and I have to pay to keep it out and away from our computers. If we don't, we should expect to budget in a new computer more often than we'd like.
3. Open emails only from people or companies you already know and with whom you do business.
4. Avoid getting and sending emails that typically have pictures and videos and links that initially show you entertaining or emotionally engaging things. The bad people know they are popular and moving and love it when you find something moving and pass it on to others in your address book. If you want to share something, share only the link.
5. When making purchases on the internet, use a one-time use, disposable charge card. Bank of America has a free "*Shop Safe*" card that generates a one-time use number that charges to your account but can't be used again. That prevents some low-paid criminally minded person working at an online retailer from writing down your number and using it elsewhere once they go home from work. Citi, Discover and MBNA are all testing controlled payment numbers. Call the customer service department of your credit card service and ask if they have any such programs.

6. If you do research on the internet (and we all do):
 - a. Use Symantec's safe browsing mode
 - b. Use the free *Tor* software that makes you and your computer invisible and untraceable
 - c. For \$79 a year, you could use *Anonymizer* <http://www.anonymizer.com/> to keep the websites from hacking into your information
7. Use a disposable email addresses that you can throw away once you've seen that a store has sold it to other scammers. Spamex.com lets you create as many temporary, disposable, email addresses as you like for about \$10 a year. If you start getting spam email to this address that you see in their "To" field, you can eliminate the address and you'll never hear from them again.
8. Be mindful that EVERYTHING you share on Facebook and LinkedIn is public forever There are programs that automatically collect your information for the day that they can use it to impersonate you and steal your money through credit and purchases.

Hope this helps.