

Bits & Bytes

Arkansas' Premier Computer Club



June 2021

Bella Vista Computer Club - John Ruehle Center

Highlands Crossing Center, 1801 Forest Hills Blvd Suite 208 (lower level), Bella Vista, AR 72715

Website: <http://BVComputerClub.org>

Email: editor@bvcomputerclub.org

COVID-19 VIRUS ADJUSTMENTS

We will continue to conduct the monthly General Meeting using Zoom over the Internet. To attend a Zoom meeting or class, you need Internet access and a device with the Zoom application installed.

We will resume some in-person classes and Help Clinics with 8 or fewer people in the Training Center, observing current masking and social-distancing guidelines.

MEETINGS

(Online) Board Meeting: June 14, 6pm,

(Online) General Meeting: June 14, 7pm, "Cutting The Cord" – another look at Alternatives to Cable TV. This will be a subset of the content from a 2.5 hour Workshop presented by the Association of PC User Groups in April.

Zoom meeting access information will be emailed to membership the weekend before and may also be found on our website. Visitors or Guests are welcome.

Genealogy SIG: No meeting (3rd Saturday).

HELP CLINICS

June 5, 9am - noon at John Ruehle center

June 16, 9am - noon at John Ruehle center

Members may request Remote Help on our website at <https://bvcomputerclub.org> at menu path **Member Benefits ▶ Remote Help** .

MEMBERSHIP

Single membership is \$25; \$10 for each additional family member in the same household.

Join on our website at <https://bvcomputerclub.org> at menu path **Get Involved ▶ Join/Renew**, by mailing an application (from the web site) with check, or complete an application and pay in person at any meeting.

CLASSES

June 22. 1-3pm Thunderbird Email Client, presented by Joel Ewing. In-person class at the BVCC Training Center. Maximum attendance 8.

Advance sign up required for each listed class: Contact Grace: email to edu@bvcomputerclub.org, text 469-733-8395, call 479-270-1643, or sign up at the General Meeting. Classes are **free to Computer Club members**. Class access information will be emailed to those signed up for the class the day before class.

Check the monthly calendar and announcements for any last minute schedule changes at <http://bvcomputerclub.org> .

NEW OR RETURNING BVCC MEMBERS

We are pleased to welcome the following new members or members returning to BVCC after an absence since last month's newsletter:

Kristy Danna

Muriel Spychala

Anita Ebert

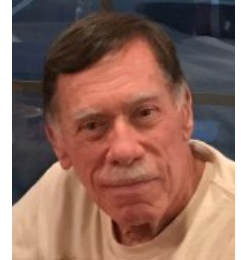
Sara Denning

Edward Wieder

Elmer Hoeffler

'TIS THE SEASON FOR FRAUDULENT EMAIL

By David Kretchmar, Computer Technician
Sun City Summerlin Computer Club
<https://www.scscc.club>
dkretch (at) gmail.com



You have probably already received emails that appear to come from a bank or other online service requesting that you verify account credentials. You might have been asked to provide personal information including account and credit card numbers and passwords. This is a standard **phishing** technique; oddly, the sender is asking for information they should already have.

“If you can’t spot a phishing email, you could be the next victim.”

Unfortunately, during the COVID-19 pandemic, we’ve seen once again that phishing lures are mutating and they’re often hard to recognize.

Phishing is a form of social engineering email attack in which the sender tries to gain access to login credentials, to get confidential information, or to deliver a virus. This is accomplished by tricking humans like you and me.

Scammers know there’s a good chance that any message will be scanned for malicious content by the security software of your browser and mail provider. Google, Edge, and most other browsers are pretty decent about stopping known spam, but plenty still gets through. Scammers are constantly changing techniques.

Since the coronavirus pandemic started to unfold, fraudsters have wasted no time in trying to profit from the uncertainty and fear connected to the crisis. In March 2020, when this all started, there was a flood of COVID-19 themed spam, spreading malware, phishing for sensitive information, or offering bogus products.



According to Google, scammers were sending 18 million phishing emails about COVID-19 to Gmail users every day in March, which Google blocked. In April Google was blocking more than 100 million phishing emails a day. And these are just the phishing emails the tech giant blocked. Yet some still

appear in your Inbox, and If you can’t spot a phishing email, you could be the next victim.

It is no surprise that the coronavirus pandemic has become a top subject for attackers. The appearance of any crisis brings new circumstances that provide a new environment for cybercriminals to innovate. At the same time, phishing attacks have also benefited from the number of new remote workers.

So how do you recognize suspicious emails?

Look at the sender email address

The sender's email address is the first place to look. If it looks "funny" or unfamiliar be careful with that message. You can check the email address by hovering your mouse over the 'from' address *but don't click*. Scammers' email addresses used to be anonymous or had very generic names with many numbers. Sometimes the sender's email address wouldn't match the sender's name or the body of the message.



Receiving emails about a problem with your account from financial institutions with whom you have no relationship is a laughable tell. But if you do get an email claiming to be from your bank, closely review the email address. The email address is sometimes the only sign of a scam, due to how professional the messages look. If you feel the email might be legitimate, check your account the way you would normally access it (not a link provided in the email).

Keep in mind that any big outfit is going to have an

anonymous address i.e., you contact PayPal at an address that includes paypal.com.

Be suspicious of attached files or unfamiliar links

Cyber criminals' emails might contain malware or send you to a malicious web destination. If you are at all suspicious, don't click. Legitimate service providers don't send messages requesting you to log in via an embedded link. Also, pay special attention to attached files – once they are opened, these attachments can install malware to give someone else control over your computer. They can then initiate attacks on other computers, including by sending spam (often infected) to every contact in your address book.

Watch for poor English

Poor grammar or words used in an unusual way are possible indications of phishing. Always be suspicious; looking for unusual language and vocabulary, or misspelled words can help prevent you from becoming the next victim. Poor spelling and other grammar mistakes are common with phishing emails that have been translated from other languages. This kind of clue is less common today because the quality of social engineering has improved, so you are likely to receive a more professional presentation. Another thing that can signal an attempted attack is generic greetings such as "Dear recipient" or "Dear friend".

There's sometimes a purpose behind misspellings and poor syntax. Cybercriminals most successfully prey on uneducated computer users, knowing them to be less observant and therefore easier targets.

Is it too good to be true or is it frightening?

Social engineering focuses on two human weaknesses, fear and greed. Does the email promise you a windfall of cash?

A blue speech bubble with a white border and a tail pointing downwards. Inside the bubble, the text reads: "Congratulations, You Have Won A Million Dollars." in a bold, black, sans-serif font.

**Congratulations,
You Have Won
A Million
Dollars.**

Does it suggest you inherited a fortune or will be paid a fortune to help someone move money out of their country? Here's an idea: Google for the same message, or a key phrase from that message. (highlight, right-click, search Google). You'll often see that many other people have received the same or similar fraudulent message.

Would-be cybercriminals using social engineering methods are very opportunistic. For example, this time of the year the names of shopping websites such as Amazon and Mayfair are used in sending out millions of emails claiming issues with your account or recent order and asking for personal information. They know consumers are most likely to have made purchases this time of the year.

The scammer wants to panic you into doing something. Don't be threatened by an email. Does the message urgently ask for help or otherwise appeal to your emotions? These are common techniques. Do not respond to an email threatening to suspend your account if you do not answer in a short time.

Homoglyph attacks

Homoglyph attacks rely on replacing characters in addresses with ones that look similar, or are the same, but belong to different alphabets. These attacks are extremely dangerous for users because there is a very limited chance of detecting the trick. Like the attack on PayPal users in which the address contained the "correct letters" taken from our Latin alphabet – with two exceptions. The attackers replaced both instances of the letter P with a "P" look-alike letter, but from a different alphabet. This "P" look-alike letter was taken from the Russian alphabet, where it is equivalent to the letter R. With this kind of attack, you are dependent on the other clues discussed in this article to protect yourself.

DESCRIBING THE QUANTITY OF COMPUTER STORAGE

By Joel Ewing, President Bella Vista Computer Club
president (at) bvcomputerclub.org
Bits & Bytes, June 2021



Computers can store data or information in a number of ways internally and on various media and storage devices. How we describe the capacity of this storage has evolved considerably over the last 70 years, which explains some of the inconsistencies found in usage.

One of the first things one used to be taught in Physics, even in High School, was that a number representing a measurement was useless (and counted as an incorrect answer) if not accompanied by the appropriate unit of measure. The unit of measure (g, kg, lb, nt, W, ft, m, km, etc.) was essential to define not only the true magnitude of the value, but to distinguish among types of measure: weight, mass, force, energy, distance, charge, temperature, etc.

How We Got Ambiguous Computer Storage Notation

While all computers in common use today tend to have storage organized around the concept of a "Byte" or "character" containing 8 "bits" (base-2 binary digits), this was not always the case. Earlier computers had organizations based on decimal digits, on characters represented by less than 8 bits, on "words" containing some number of decimal digits (10), or on "words" containing some number of bits (12, 16, 32, 36, 48, 60).

For computers organized around decimal digits with memory locations addressed in decimal, one talked about memory having so many "K" digits or words of memory, where "K" was "1000" (no computers had enough memory yet for "M" to be an issue). If varying amounts of memory could be purchased, the physical memory sizes had to be manufactured in quantities that were round numbers in base-10. Machines with 20,000, 40,000, or 60,000 digit memory were described as 20K, 40K, or 60K machines.

Computers that were not organized around decimal digits addressed internal memory locations using a binary address¹, and this required that memory be manufactured in quantities that were round numbers in base-2. So you would have memory size increments of 1024 (2^{10}), 2048 (2×2^{10}), 4096 (4×2^{10}), 8192 (8×2^{10}), 16384 (16×2^{10}), etc. Those that worked with such computers quickly tired of describing computer memory capacity in the cumbersome exact-decimal-value notation and adapted the shortcut of using $K=1024=2^{10}$ so the above round numbers in binary could be expressed more simply as 1K, 2K, 4K, 8K, 16K. This was particularly convenient, since even if your mind subconsciously saw these values "in decimal", you would only be off by 2.4%. Note that although this is a convenient notation, it is a "corrupted" usage of "K", which is a prefix derived from the Greek word for "thousand".

Computer storage other than central internal storage was a different matter. Disk storage and tape storage capacities were based on state-of-the-art recording techniques, choice of physical media dimensions, and recording densities. These factors produced capacities which tended to not be nice round numbers in either binary or decimal. Changing the definition of "K" in this context provided no notational simplification, so in the context of disk and tape capacity "K" continued to have its customary meaning of "1000".

As maximum available and affordable computer storage capacities increased, the above conventions were extended to include the prefixes of

- M (mega), meaning $10^6 = 1,000,000$ OR $2^{20} = 1,048,576$, depending on context
- G (giga), meaning $10^9 = 1,000,000,000$ OR $2^{30} = 1,073,741,824$, depending on context
- T (tera), meaning 10^{12} OR 2^{40} , depending on context .
- and so on, for prefixes for powers of 10^3 higher than 10^{12} .

Up until the mid 1980's, the only people exposed to this prefix usage were the relatively small number of computer professionals who understood the conventions. The vast number of PCs and other computer devices that have become available over the last three decades have resulted in many computer users now being exposed to these conventions without the underlying knowledge of computer architecture to understand the context distinctions.

1 An exception were some ingenious machines created at Moscow State University starting in 1958 ("Setun" and "Setun 70") based on the ternary (base-3) number system rather than binary. The ternary design required fewer discrete electronic components, a distinct advantage because of electronic component scarcities in the Soviet Union at that time. Soviet internal politics and software compatibility issues with the more-widely-adopted binary architectures caused the eventual demise of this architecture.

The Solution

To eliminate this decimal/binary ambiguity, in December 1998 the International Electrotechnical Commission (IEC) approved an International Standard for names and symbols for prefixes for binary multiples for use in the fields of data processing and data transmission. That standard is recognized by NIST (U.S. National Institute of Standards and Technology – formerly known as the US Bureau of Standards) and can be found at <https://physics.nist.gov/cuu/Units/binary.html>

By this standard, usages of prefixes K, M, G, and T where a power of 2^{10} is intended should be replaced by Ki, Mi, Gi, and Ti respectively. These abbreviations correspond to **kilobinary**, **megabinary**, **gigabinary**, and **terabinary**, and are pronounced as "kibi", "mebi", "gibi" and "tebi". So, 16 GB of RAM for a PC should more correctly be called 16 GiB of RAM. This would be spoken as "16 gibibytes", and mean 16×2^{30} .

Getting people to adopt the newer non-ambiguous conventions has been a non-trivial exercise. After two decades, retail consumer hardware manufacturers are still frequently not observing it. You will find some computer software correctly using the new standards (system and file utilities in Linux), and some not (system and file utilities in Windows 10, which tends to report both RAM storage and Disk storage in "GiB", with both mislabeled as "GB"). That consumers are confused is evident when you see someone who erroneously believes that "GB" always means 2^{30} for computers, or is just confused by Windows 10 misuse of "GB", complain that the capacity of his hard drive was exaggerated because he misinterpreted the manufacturers 500 GB to mean 500 GiB. I personally try to use the standard binary prefixes consistently where appropriate, both to avoid unnecessary ambiguity and to educate others about their existence.

If you are familiar with the conventions, it is clear when a retail PC advertises a RAM memory of "8 GB" that what they really mean is "8 GiB", because PCs use a computer architecture with binary memory addressing. It is similarly clear that a mechanical SATA Hard Drive advertising 1 TB of storage probably means it is close to, hopefully a little over 1TB, and not 1 TiB, which would be 10% larger. Close but not exact, because there is no reason why a physical device with varying physical track lengths should hit a capacity with a nice round decimal number.

Now in the case of a "240 GB" SSD solid-state drive, I'm not certain what value is intended. Since there is discrete solid-state memory under the covers, no doubt the base storage inside the unit is really 256 GiB. But there also has to be a programmed computer processor inside that is emulating a SATA hard drive, so out of that 256 GiB some memory must be used for the hard drive controller program, and some space taken for buffers and other data storage required for the hard drive emulation, and perhaps some space kept in reserve just in case marginal performance or failures are detected in some blocks of the memory, like having hidden alternate tracks on a mechanical hard drive that can transparently replace a failed physical track. After deducting the overhead for the device emulation, that could leave either 240 GB or 240 GiB usable storage for the emulated hard drive. I suspect they would mean the lower 240 GB in keeping with mechanical hard drive capacity conventions, but I'm not 100% sure.

It ought to be possible to get RAM and PC manufacturers to use the more correct GiB in place of GB for RAM capacity. Hard drive and SSD manufacturers should specify their approximate capacity in both GB and GiB as well as the actual exact Bytes. While the current GB values are conventional usage, you still have the problem with neophytes seeing only a GB value and thinking it should be interpreted as GiB.

Another sloppy usage which drives me to distraction is hearing or reading someone describing his computer storage or speed as so many "gigs". So he has "billions". Billions of WHAT? "G" is only a quantity multiplier, not a unit of measure! Without the correct units the number is meaningless. This misuse is particularly confusing in the area of data transmission speeds, where units of both "bits per second" and "Bytes per second" are in common use.