— The DataBus —

Monthly Newsletter of

The Dayton Microcompter Association

Volume XI (New Series) № 10 (Octobber 2021)

Special Cybersecurity Issue

—Contents—

Save a Tree (or at least a branch)! If you prefer to print your DataBus rather than read it directly from a monitor, don't print page 20 unless you need to renew your membership.

DMA™

Post Office Box 4005
Dayton, Ohio 45401
(937) 777-DMA1
(777-3621)

Visit us at:
DMA1.org

Established in 1976, DMA is a group of Dayton-area professionals and enthusiasts in the field of computing and digital information technology. General Membership Meetings are usually held on the last Tuesday of each month. DMA has a number of Special Interest Groups (SIGs) in areas ranging from digital investing and genealogy to the Linux operating system. Each SIG meets according to its own schedule. DMA is a member of the Association of Personal Computer Users' Groups (APCUG) and the Affiliated Societies' Council (ASC). Click on any of the logos—including our own (top left)—to go to that organization's Web site.

apcug
An International Association of Technology & Computer User Groups

Submissions …

The DataBus welcomes compliments, complaints, suggestions, and especially articles. We can accept articles in ASCII, or as attachments in plain text, Microsoft Word, Open or Libre Office Writer, or, yes, even in WordStar (a word-processing program that goes back to about 1980!). Send articles to:

Editor@DMA1.org

All articles are subject to editing for spelling, grammar, usage, and space. Retain a copy of your work, as The DataBus cannot be responsible for loss. When articles are of roughly equal quality and importance, those by paid-up DMA members receive preference.

All registered trademarks, for example: the DMA Arrow, APCUG, Amazon Sidewalk, Hulu, Netflix, Windows, WordFence, or Zoom, are the property of their respective owners. However, the Registered Trade Mark symbols (® or ™) have been omitted for better readability. The Editor occasionally inserts comments into articles. Such comments are sometimes preceded by the phrase: "Editor's Note," are often in square brackets [like these], and are always in sans-serif type, like these paragraphs.

The DataBus is written and published by volunteers. We do not give professional advice on hardware, software, or network installation, repair, security, or troubleshooting. If you need expert assistance for your digital device or network, please seek the advice or services of a qualified professional.

October Meeting: *7 P.M., Tuesday, the 26TH*

No Driving—No Parking—No Charge*

* This is a "hybrid" meeting: via ZOOM, but also in person. Come at 6 P.M. if you wish to join us in person for dinner at T. J. Chump's Restaurant in Huber Heights, next door to the Meijer's Supermarket. Click *here* for a map. The restaurant has free parking. It is also accessible via RTA bus routes 18 and 19, but there is a short walk from the bus stop in the Meijer's parking lot to the restaurant.

Gary COY: *Cybersecurity & You*

If you come in person, join us at 6 P.M. for dinner.
The Main Meeting starts at 7 P.M. via ZOOM.

Cybersecurity and You

Presented by **Gary Coy**

CYBERSECURITY AWARENESS MONTH is observed every October. Created as a collaborative effort between government and industry, it tries to ensure that *every* American has access to the resources we need to stay safer and more secure on-line. Now in its 18th year, Cybersecurity Awareness Month is co-led by the National Cyber Security Alliance (NCSA) and the Cybersecurity and Infrastructure Agency (CISA).

https://staysafeonline.org/

It is essential for anyone using e-mail, a browser, social media, or any device with internet access, to have an understanding of the basics of cybersecurity. Tonight's presentation will be a refresher on cybersecurity awareness. The security enhancements of Windows 11 will also be covered.

Gary Coy is our newly elected DMA president. He has worked in the electronic and computer industries for over 20 years, while at the same time running a computer repair business. He has been a member of DMA for over 10 years, serving as an officer, trustee, and frequent presenter. Gary is currently VP of the NASAC computer user group in Xenia, Ohio. He currently works for the Speedway Corporation where he started as a repair technician and now holds the position of customer service claims specialist. Gary also serves his community as a volunteer and part-time EMT.

Our meeting starts at 7 P.M. DMA members will receive an invitation by e-mail for Zoom. Others may request an invitation using …

http://www.dma1.org/contact-us/

Or … join us in person at T.J. CHUMP'S, 7050 Executive Blvd, Huber Heights OH. Click *here* for a map. There's free parking. Chump's restaurant is also accessible via public transit: RTA Bus Lines #18 and 19. Click here for the Route 18 weekday schedule, and here for the Route 19 schedule. (A short walk across the parking lot of Meijer's Department Store is necessary.)

… TDB

Minutes are normally published almost two months late, because the Minutes for, say, the September Board meeting must be approved by the Trustees at the *following month's* meeting — in this case, early October. The corrected and approved August Minutes would thus appear in the October DataBus (this issue), published toward the end of the month.

Trustees' meetings are on the *first Monday of each month,* except when that day is a legal holiday, for example: Labor Day in September. During the epidemic, Trustees began meeting via Zoom. This was so successful that they have decided to continue the practice indefinitely. Meetings begin at 7 p.m. and are open to all DMA members. Request Zoom credentials (that's a fancy way of saying "an invitation") from Secretary Glady Campion at the October General Membership meeting.

DMA Board of Trustees

MINUTES — Meeting of Monday, September 13, 2021

CALL TO ORDER

The meeting was called to order at 7:05 p.m. by Peter Hess, via Zoom.

Trustees present: Martin Arbagi, Glady Campion, Edwin Davidson, Pat Flynn, Peter Hess, and Ed Skuya. **Excused**: Chester Howes. **Absent:** Ken Phelps**. Guests:** Mark Camden.

OFFICERS' REPORTS

President – Ken Phelps

No report.

Vice President – Peter Hess

Gary Coy gave a good presentation on Amazon Sidewalk. There has been plenty of interest in this new technology and his talk was very informative.

Peter mentioned that he will need to cut back on the time he spends with DMA due to other new responsibilities.

Secretary – Glady Campion

Glady presented Minutes for the August board meeting. Martin Arbagi moved the Minutes be accepted as corrected. Edwin Davidson seconded and the motion passed with Glady abstaining.

Treasurer – Pat Flynn

Pat presented a report for August.

COMMITTEE REPORTS

Audit – Glady Campion

In progress

Fundraising – Peter Hess

Peter is still working on finding out more about Network for Good. He is also talking with Kroger and Dorothy Lane Markets about their rewards programs.

—Notice—

Because of confidentiality concerns (hackers could readily discover in what financial institutions DMA holds its assets), Treasurer's Reports will not be published hereafter. However, account balances are available to DMA members on request.

(Continued on page 5)

(September Minutes—Continued from page 4)

The Dayton Foundation told Peter they will accept credit card donations for DMA through their website and will contact us if offered other types of donations. Once activated, a link on the DMA website will bring up a page on The Dayton Foundation website where the donor can enter a credit card number and specify how the donation is to be used. TDF has a Donor Express page that provides each fund owner with easy access to information about their fund.

Marketing – Edwin Davidson, Pat Flynn, Peter Hess, Debra McFall

Peter sends out over 35 press releases each month.

Membership – Glady Campion

As of the end of August, we had 48 Regular, 4 Associate, 0 Student, and 5 Life members for a total of 57. Attendance was 29, including 16 who attended in person at TJ Chumps.

Prizes: Edwin Davidson selected the Kensington Pro Ergo Keyboard. Eric Ottoson asked for the Amazon Echo Dot. Ken Phelps snatched the PNY 256GB 3.0 Flash Drive. Kathleen Kannik chose the Solo New York 15” laptop sleeve.

Net Administration Team – Ken Phelps, Gary Turner, Pat Flynn, Brent Kerlin, Mark Camden

Mark e-mailed the Trustees a report by Wordfence on the security of our website, reporting no threats.

Peter e-mailed a revised version of a “DMA Needs” page to the Trustees and asked Mark to post it to the website. Mark placed a link to this new page on the “About” page of the DMA Web site. This page includes a request for donations through The Dayton Foundation and a request for volunteers.

Programs – Peter Hess

Many thanks to Gary Coy for his talk on Amazon Sidewalk, how the Sidewalk enabled devices use a mesh network to deliver services, and how these products are designed to protect users’ security.

September — MetroNet will give a talk on gigabit fiber internet.

Peter is still trying to get a speaker from Generac.

Other suggested topics: Ransomware, Deep Fakes, Streaming video, Car hacking, Chromebooks, Bitcoin and Block chain, InitiativeQ.com, Data.ohio.gov, converting laptop to Chrome

Publications – Martin Arbagi

The August issue of The DataBus was posted to the Web site.

UNFINISHED BUSINESS

Wright State Archives – Martin Arbagi, Glady Campion

Still in progress.

Next Board Meeting

Next Board Meeting will be 7:00 p.m. on Monday, October 4, 2021. We will continue to use Zoom.

Fairborn Fire Station #2 is reserved through December 2021.

List of DMA accounts – Glady Campion

Glady is continuing work on a list of all accounts currently held by DMA.

Summer Picnic – Glady Campion

Our picnic was held Saturday, August 28, at Shellabarger Park in Riverside. There were 32 people who attended. Although the weather was hot, we thankfully had a good breeze run-

(Continued on page 7)

Have a business card? Are you a DMA member?

Any paid–up member of the Dayton Microcomputer Association is entitled to a *free* business card–sized advertisement in The DataBus. Send a good–quality image (600 dpi or better) to Editor@DMA1.org, or give your business card to **Martin Arbagi,** the Editor, at any DMA meeting. We can embed a link to your Web site (if you have one) within the image of your card. Under weird IRS regulations, your Web site may not include discount coupons for DMA members, although discount offers may be included in the advertisement *itself.*

☺ Help DMA by using Amazon's Smile program! ☺

Amazon, the Internet's largest retailer (if you haven't noticed, Amazon isn't just for books any more!) has a "Smile" feature whereby Amazon donates a percentage of almost any purchase you make to a selected nonprofit organization. There is *no* extra cost to you. Click *here* to learn more or *here* to go directly to the sign-up page. Be sure to put DMA down as the beneficiary of your purchases.

(SEPTEMBER MINUTES—*Continued from page 5*)

ning through the shelter. Everyone took home some great prizes. Several people also picked up items from the pile of pre-owned hardware giveaways. The leftover giveaways were offered to Dayton Diode and the few unwanted items went to Goodwill.

NEW BUSINESS

Use of the DMA Zoom account – Peter Hess

Edwin Davidson asked to use the DMA Zoom account for a group he belongs to that meets the 3rd Tuesday each month. Peter already granted Gary Turner access to the Zoom account for a group he belongs to that meets at noon once a month. None of the Trustees voiced objections.

VOLUNTEER OF THE MONTH/QUARTER/YEAR

Edwin Davidson moved that **Glady Campion** be nominated Volunteer of the Month for her work on the Summer Picnic. Ed Skuya seconded and the motion passed with Glady abstaining.

ADJOURNMENT

Pat Flynn moved to adjourn at 9:10 P.M. Edwin Davidson seconded and the motion passed.

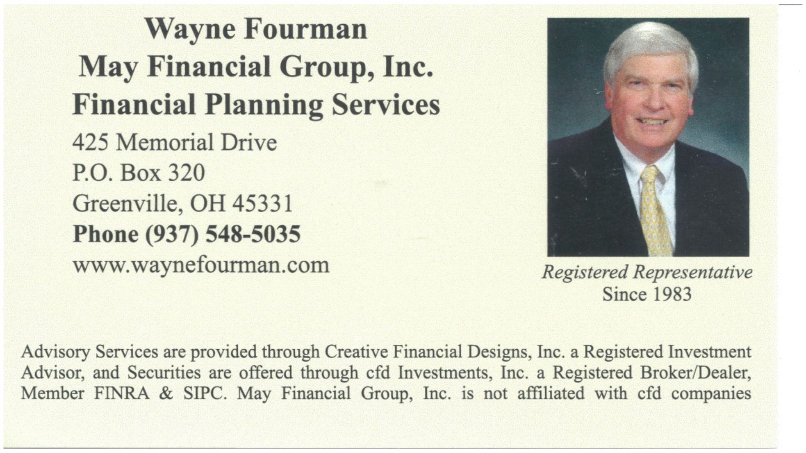
Respectfully Submitted,

Glady Campion, Secretary

(IDENTITY THEFT—*Continued from page 18*)

- Put a credit freeze on your accounts with credit bureaus: Equifax, Experian, Innovis, TransUnion
- Protect your social security number – only give it out when absolutely necessary.
- Be aware of billing cycles – if financial information is late or doesn't come, follow up
- Be cautious of participating in viral memes such as "name your most memorable concert."
- Set strict privacy settings on Facebook, Twitter, Pinterest, Instagram, and LinkedIn

If you are a victim of identity theft, report it to the FTC online and create an account to create a report and generate a recovery plan. You will gain access to recovery plan updates and prefilled form letters to send to creditors. You should also report medical identity theft to



Wayne Fourman
May Financial Group, Inc.
Financial Planning Services
425 Memorial Drive
P.O. Box 320
Greenville, OH 45331
Phone (937) 548-5035
www.waynefourman.com

Registered Representative
Since 1983

Advisory Services are provided through Creative Financial Designs, Inc. a Registered Investment Advisor, and Securities are offered through cfd Investments, Inc. a Registered Broker/Dealer, Member FINRA & SIPC. May Financial Group, Inc. is not affiliated with cfd companies

↓ Patronize Our Member–Advertisers! ↑

GARY'S COMPUTERS
Computer repairs,
upgrades, & custom builds.
Home networking.

GARY COY
Computer Technician

4946 Peacock Road
Springfield, Ohio 45502
937-360-1464
gcoy@woh.rr.com
In-home services available

Travel Through Time On Indiana's Most Scenic Railroad
WHITEWATER VALLEY RAILROAD
765-825-2054
www.whitewatervalleyrr.org

Have you heard....?

Compiled from various sources

Flying car companies in Ohio

Half a dozen companies have set up shop in southwestern Ohio. They are not the first. More than 500 companies are already working in the field. Technically, these vehicles are referred to as eVTOL – Electric Vertical TakeOff and Landing. Much of the development is located near the Springfield Beckley Municipal Airport and Wright Patt. The first flying car to arrive in Ohio was the HEXA by LIFT Aircraft. The aircraft's ultra-light designation means it does not require certification from the FAA and does not require a pilot's license to fly. Air Force Colonel Nathan Diller hopes to someday use flying cars to transport troops and medevac wounded personnel.

Autonomous deliveries

Walmart is partnering with Ford and its self-driving unit, Argo AI, to deliver on-line orders to customers' homes. Argo AI has been testing autonomous vehicles for a while in Miami, Austin, and Washington, D.C. The cost of autonomous delivery is said to match regular rates, with initial deliveries to begin later this year.

Walmart is also working with a startup called Gatik to use autonomous box trucks to make deliveries in Arkansas starting sometime this year. And if all goes well, Walmart plans to remove the safety driver from the box trucks next year.

Last week, FedEx announced its first autonomously-driven tractor trailer delivery route. It has been working with truck maker PACCAR and self-driving company Aurora, which is backed by Amazon. FedEx will start making deliveries in Texas along Interstate Highway 45 between Houston and Dallas with a safety driver behind the wheel.

Cryptocurrency Crackdown in China

After the latest ban, over $400 million worth of tokens were liquidated within 24 Hours. Tightening of Chinese regulations on trading and minting of cryptocurrencies already caused a crash in April and May. This latest round of crackdowns has pushed the market into the red. Chinese regulators imposed a blanket ban on all cryptocurrency transactions and mining in the country last week. Top currencies such as Bitcoin and Ether have lost significant value. The People's Bank of China made crypto-trading illegal and said it planned severely to punish anyone doing it.

(Continued on page 10)

(Digital Whispers/Have You Heard?—Continued from page 9)

World Robot Conference, Sep 10-13

This conference in Beijing offered visitors a look at more than 500 robots exhibited by some 110 companies. A Chinese-speaking “Albert Einstein” stole the show on the first day. According to reports, it is one of the most intelligent androids ever developed and communicates fluently in Mandarin. The lineup included everything from industrial assembly line robots to humanoid servants and machines capable of performing surgery. There were several models of dog robots, some climbing stairs and others doing back-flips. Some visitors played with large Koi (goldfish) swimming in a pool of water while others were distracted by a life-sized robotic shark. A human-sized panda demonstrated its ability to walk and do Tai Chi. WRC has been held annually since 2015.

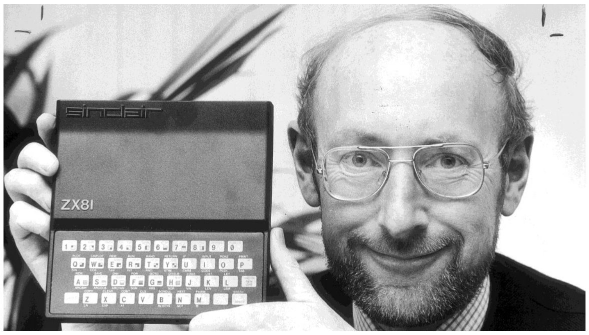
www.WorldRobotConference.com

Reality TV is heading for outer space

Two upcoming reality television shows plan to offer a once-in-a-lifetime grand prize: A trip to space. Mike Massimino, a former astronaut and former guest star on Big Bang Theory, talks to CNN Business about the feasibility of these shows’ taking off.

https://www.cnn.com/videos/business/2021/08/04/filming-in-space-reality-television-orig.cnn-business

Sir Clive Sinclair



The British inventor, who helped popularize personal computers, died this month at age 81. His first personal computer, the ZX80, was a steal at $200. This invention was one of the devices that helped bring computing into homes everywhere. Most of his inventions hinged on making existing products smaller and more affordable. The ZX81 was priced at only $100 and more than 1 million were sold. Sinclair stunned a reporter from the *Guardian* in 2010 when he said he didn’t use a computer. Sinclair said, “Sheer laziness, I think”, “I can’t be bothered”.

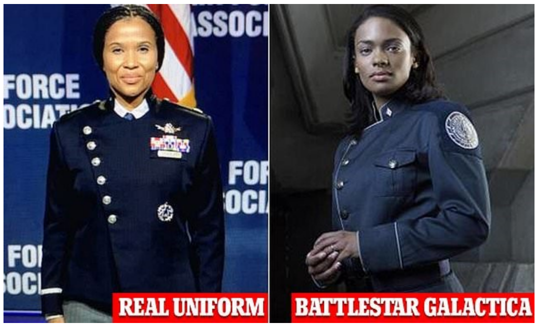
https://www.cnn.com/2021/09/17/tech/clive-sinclair-death-zx-computer-cec/index.html
http://oldcomputers.net/zx80.html

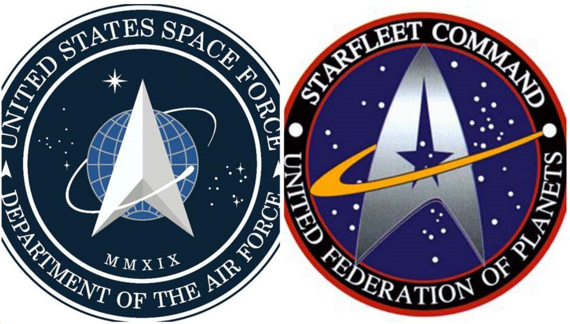
US Space Force Trappings

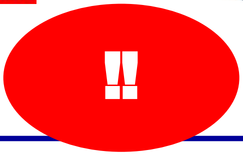
Still in its infancy, the United States Space Force, which was announced in 2019, has become a target of jokes by many on the Internet, even inspiring a Netflix comedy series. The proposed uniform designs unveiled last week were seen as much too similar to those from the TV series, *Battlestar Galactica.* The Space Force emblem is nearly identical to the Starfleet logo from S*tar Trek* — so much so, it’s a wonder Paramount didn’t sue the USSF. Learning that Space Force personnel are to be called “Guardians” sure felt like an appeal to the *Guardians of the Galaxy* fan base. Hope is that the USSF’s mission will be far more “down to earth!”

(See illustrations on page 11,)

(*Digital Whispers/Have You Heard?—Continued from page 10*)




UNITED STATES SPACE FORCE
DEPARTMENT OF THE AIR FORCE
MMXIX
STARFLEET COMMAND
UNITED FEDERATION OF PLANETS



DMA Events for Oct 17 – Nov 20, 2021

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
Oct 17	Oct 18 **Apple Dayton** CANCELLED	Oct 19	Oct 20	Oct 21	Oct 22 **Python Self-Study** Noon, Online See http://d8ndl.org	Oct 23
Oct 24 	Oct 25	Oct 26 **MAIN MEETING** 7:00pm Online -AND- TJ Chumps 7050 Executive Blvd Huber Heights	Oct 27 *My*	Oct 28	Oct 29 **Python Self-Study** Noon, Online See http://d8ndl.org	Oct 30
Oct 31 	Nov 1 **DMA Trustees** 7:00pm Online	Nov 2 *Election Day* 	Nov 3	Nov 4 **Genealogy SIG** Restarting Online	Nov 5 **Python Self-Study** Noon, Online See http://d8ndl.org	Nov 6 **Classic Computers** 3:00pm By phone
Nov 7 *Daylight Savings* 	Nov 8	Nov 9 **Investment SIG** 7:00pm Online Investment_sig @dma1.org	Nov 10 **Dayton Dynamic Languages** 7:00pm Brixx / online http://d8ndl.org	Nov 11 *Veteran's Day* **NASAC** 6:00pm Xenia Library	Nov 12 **Python Self-Study** Noon, Online See http://d8ndl.org	Nov 13
Nov 14	Nov 15 **Apple Dayton** CANCELLED	Nov 16	Nov 17	Nov 18 **Linux SIG** 7:00pm 348 Russ Eng Wright State Univ. Colonel Glenn Hwy Beavercreek	Nov 19 **Python Self-Study** Noon, Online See http://d8ndl.org	Nov 20 **Classic Computers** 3:00pm By phone

PASS(word) The Beef, the Hash, the Salt for Einstein, and a Dictionary

By Arthur Gresham, Editor, UCHUG Drive Light
Under the Computer Hood User Group
www.uchug.org
1editor101 (at) uchug.org

Passwords and Hash, Part 1

The Meeting

At the September 2021 UCHUG General Meeting, the two primary presentation topics were closely related in the area of Security: SMISHING and 2FA. In addition, and coincidentally, October is National Security Awareness Month.

Discussion after the presentations moved into questions concerning the passwords we use on all the sites and services of the Internet. Attendees shared several questions and opinions about managing passwords, how to build passwords, security of passwords, and the impact of losses from the frequent data breaches on small and large businesses, government, or anyone else operating a Web site using password technologies, resulting in having sensitive information stolen.

The Beef

Several issues were raised in that meeting, questioning the validity of secure password methods, ease or difficulty of hacking into some system with or without an individual's true password, difficulty of "cracking" someone's individual password, or many passwords in a system data base. We did not all agree and had some small but lively BEEF.

Obviously, there are many well-trained specialists in this area responsible for creating secure methods and protecting systems from the loss of your password. But many of the methods used are not easy to understand and involve sophisticated mathematics. As a result, there are a lot of myths and misconceptions about how passwords are stored by a corporation (or Web site) and how one could go about getting a password (in particular, *your* password) from that collection of thousands. For example, how can a password be cracked? Or hacked? Or unencrypted?

The Banker

But let's go back in time to basics: to the good old days when taking your money to the bank was a face-to-face activity. You walked up to tellers (remember when live people did that?) and handed them your bank passbook. Then you gave them your money.

They opened a big ledger, turned a few pages, and wrote your deposit into your account. How did they know to what account to credit the money? Answer: the tellers looked up your account number in the passbook with *your* name on it.

How did they know it was really *your* account? Simple: you have a face, which they recognized (you both were members of the same Grange Hall, or perhaps they had voted for you as Mayor or shopped, in your general store). Plus, you had "the passbook."

Your USER ID was the account number written in the passbook (physical possession); your Password (only you have it) was your face (a Biometric Password — aka Facial Recognition) — The Original Two Factor Authentication (2FA)!

The Data

Fast forward to today, and no one is storing your information in plain writing in a big

(Continued on page 13)

(PASSWORDS—Continued from page 12)

ledger. Instead, your valuable information, pictures, account balance, or credit card numbers are all stored as ones and zeros on a computer somewhere. Typically, most of this information is organized in huge data bases or files. Some parts of it can be in plain language because it is simple information. However, the parts that give it security from theft should be protected somehow.

That is what happens with your password. When you create a password on a Web site, that password isn't stored verbatim on the Web site's server. That's because your password could be published and made freely available (the trade term is pawned)[1] if the server's security were compromised. We call that a "data breach."

Instead, your password is put through a process called "hashing," which significantly improves security (provided your password is strong enough). In addition, the data base record to access *your* account will now have:

- ✓ Your USER ID = this could be your e-mail address or other name you use as the first entry in your login
- ✓ Your HASHED password = you must enter a password to verify that they match
- ✓ Your name or other information, which may be encrypted, or plain text
- ✓ Your account number or other internal ID of your account
- ✓ Other data about your account, such as answers to your security questions, preference settings you have made, or any of the other many things that you set up for your use of that on-line space.

The Hash

There are more than fifty Hash Programs. The most popular are MD5, SHA-1, SHA-2, SHA-256, NTLM, and LANMAN.

> Hashes are the output of a hashing algorithm like MD5 (Message Digest 5) or SHA (Secure Hash Algorithm). These algorithms essentially aim to produce a unique, fixed-length string – the hash value, or 'message digest' – for any given piece of data or 'message'.[2]

Using a complex algorithm, hashing turns your password (or any other piece of data) into a short string of letters and numbers. (3) It is a short "indicator" of the original text. (Note that hashing algorithms are *not* compression applications such as ZIP files that errorlessly retain all the original content. I will discuss this in detail in Part 2.)

If a Web site or corporation is hacked, the hackers don't get your password. Instead, they just get access to the database with the encrypted "hash" created by your password.

A common hash application is MD5, which returns a 32-character string from any input. Below are a few examples of what a hash looks like:

md5(*helloworld*) = fc5e038d38a57032085441e7fe7010b0
md5(*hell0world*) = 0a123b92f789055b946659e816834465
md5(*g84js;l238fl-242ldfsosd98234*) = 42e7862f4ad5225471866d2023fc4cca#
md5(*helloworld*) = fc5e038d38a57032085441e7fe7010b0

The Recipe for Hash

From the examples above, notice these things are always true; they are in every recipe:

- ✓ **Small changes matter a lot** – Take a look at examples 1 and 2. Just *one* digit has been altered, from an "o" to a "0." (OH to ZERO.) This is a very small change, and yet the second output is unrecognizable from the first.

(Continued on page 14)

(PASSWORDS—Continued from page 13)

- ✓ **The output length never changes** – The input in example 3 is considerably longer than the other examples, yet it produces an output of the same length (32 characters). You could input an entire book into the MD5() hash function, and you would *still* get a 32-character string as the output.
- ✓ **Repeatable** – An input will always give the same output when hashed using the same function. If this weren't the case, they would just generate a random output, which would be useless for passwords. (I included the same function in example 1 as example 4 just to see if you were paying attention.)
- ✓ **Hard to reverse** – Even though a hacker may be able to tell the function used to create a hash, it's impossible to reverse that function and generate the password. In fact, it's so hard that trying millions of combinations to try and produce the same end result (a brute force attack) is typically quicker than the calculations required to reverse the hashing process. (The Humpty-Dumpty Rule: You can't uncrack the scrambled egg in the HASH — more about that later)[3]

Einstein Expects Results

As mentioned in item 3 above, we *expect* to get the same results for a given string every time. To get anything different would be crazy. That is what we count on for this concept to work, and we will also see later why it can be dangerous if you use a short password. [EDITOR'S NOTE: The Author, Mr. Gresham, is referring here to a quote attributed to Albert Einstein: "The definition of insanity is repetition of the same action again and again, expecting a different result." There is no evidence that Professor Einstein said any such thing.]

So, let's follow the steps in a normal log-in.

STEP 1 – A user visits a new site, fills in a form to create his (or her) user name, uses a given default, and then creates a password.
STEP 2 – That password is put through a hash function, and the hash is stored in the company's data base.
STEP 3 – Later, when a user logs in, he enters his password.
STEP 4 – That password is run through the same hashing function as was used before.
STEP 5 – The server checks this hash against the one stored for the user in the data base.
STEP 6 – If the two hashes match exactly, the user is granted access.

The Dictionary for Uncracking the Egg

So, if no one can unscramble the password, how are the criminals actually getting into an account after getting that Data Breach file from the Dark Web? The answer is they probably don't need to unscramble it. They have a Dictionary — or several. I am referring to what is properly called a "Hash Table Dictionary" (also known as a Rainbow Table. (4) I will simply call it … a dictionary.

What is a dictionary, and how does it help? Remember in "The Hash" that the data for account 1 and account 4 had an identical Password and Hash? THAT is the weakness of a hash code. Anyone can run the hash function on as many words as they want and save the hash values to a data base (this becomes their Dictionary). SO, they can save the hash for all the pass-

(Continued on page 15)

(Passwords—Continued from page 14)

words like “2345” and “admin” and any other word in a list of well-known, commonly re-used, and very bad passwords.

For example, the MD5 hash for *helloworld* is

fc5e038d38a57032085441e7fe7010b0

And, that PW is now in the hackers’ “dictionary.” When they look for “fc5e ...” in the stolen data base, they find it, and it belongs to both user 1 and user 4. Both must have a password of *helloworld*. Almost zero seconds to look through the data and find all the fools who have used *helloworld* as their password. And the hackers are not even breaking a sweat yet.

So, if you are a bad guy, what do you do? You would create huge lists using all the known passwords and their hash. Those lists of words and phrases contain things that have been used most often that will give them the biggest bang for their buck. And, with the hash for each of those passwords, all you need to do is look for them in the stolen data base. Just one problem, and it is a big one; there are a lot of words you must hash. That creates huge files. (You can check any password, plus variations, in a list of 14,344,391 known passwords. For example, Google for “hello kitty” at this site:

https://md5hashonline.com/most-common-passwords/

Hint: On page 310 it is word number 30,972)

Bigger is Better

And the longer the password lengths get, the huger (more bigger?) that file grows. For example, the number of passwords that could be formed with just nine lower case letters *(abcdefghi*) is 5,646,683,826,134. But, of course, all those are not words, and as the number of characters (or numbers or symbols) increases, so does the size of the data base hackers must hash to complete their dictionaries. So even if they had a data base with all the possible combinations of nine lower case and three upper case letters, they would have almost 4 x 10^{20} passwords. *And* with no symbols or numbers, it is not even close to being complete. *And* they would need to buy a lot of big drives and have lots of supercomputers working around the clock.

So what do they do? They have reasonably sized (but nonetheless huge) Hash Table Dictionaries, which they can afford to purchase, and have enough disk space to store, to get maybe just those top 5 (or 14 or 600) million common, repeated, very awful, known passwords.

But wait ... There’s more. We have only done that for the MD5 function. The hackers still need the time and disk space for the SHA-1, SHA-256, NTLM, and LANMAN apps. And what about words written in other languages? (*Holamundo* is *helloworld* in Spanish!) More possibilities. Without those, all of the data that was breached is of much less use to them. Unless they want to test words one hash, one at a time, that is called Brute Force. For the next 10 thousand years. (See footnote 6 about Hashcat). It is possible, but.....?)

To Improve the Hash, Add Salt

So, you see the problem here. Einstein told us. [Editor: No he didn’t.] Do the same thing, get the same thing. It *is* repeatable. Those repeated passwords all had the same repeated hash. How can that be fixed? It is neither impossible nor difficult. It can and should be fixed from two ends of the system.

If the hash is bad, we need to add Salt. But who should add the salt, You, or the Cook? It turns out the Cooks ought to season the hash, but in case they did not, then you should.

(Continued on page 16)

(PASSWORDS—*Continued from page 15)*

Let the cook add the salt.

In this case, the "cook" is the guy in the IT shop who wrote the hash routines and saved the password you entered. Salting is adding something to the hash to make it different. For instance, adding the word Salt to *helloworld* and then hashing *helloworldSalt* **or** *Salthelloworld* will generate new, unique hash values. This is good.

Here is how it works. (And I am going to shorten the hash just to make this readable)

If *helloworld* = fc5e0380 then *helloworldSalt* = er8d25a9

Now when hackers look for fc5e0380 (the word in their standard password list), they will not find it.

The bad guys will have to re-do their entire hash table dictionary if cooks add the same salt to every word when they hash it. Thus, more time is added, delaying access, and costing the hackers money.

But the better site managers change the Salt shaker on every item. So the Salt can (must) be different (random) for every single entry in the database. This really disrupts the hackers' day because they must re-hash every standard password with every salt — effectively impossible.

Using our example, we could have three customers with the same password but now (salted with 'Salt,' '69b21' and 'pqv42')1 helloworldSalt = er8d25a9

2 helloworld69b21 = a6d51cbc
3 helloworldpqv42 = f56702622

Now no matter what the hackers have in their dictionary for *helloworld*, they can never find it in the target file.

For more about Salting, plus a very excellent description of the Dictionary process I have described, you should read at

https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/

Salt it yourself

But wait, you say. I do not know if that site is using Salt (and no one should ever answer that question about their data). So, what can you, as the customer do? Bring your own Salt!

Salt all your passwords. Use whatever trick works for you to add your special something to *every* password you create.[4]

Also, if you use a short-length Master password[5] for your Password Manager, Salt it too. (Or better yet, make it a long, easy phrase.) Simply add Salt when you type it in. Now, if anyone finds that sticky note that says your password is "Arenteyespecial?" he will get nowhere without your special seasoning. (And no, don't write your salt down next to the beef.) And for all the passwords in your Password Manager, store them plain, and add the Salt during your login, and no one will ever know. If your plain character passwords are ever compromised, none of those passwords will work. Frustrating the bad guy, saving your bacon (and everything is better with bacon).

Some lessons learned:

- ✓ Always Use a Password Manager program or app with a *long* master passphrase
- ✓ Create a long and seemingly *random* password for every site (easy to do with most Password Manager programs/apps)
- ✓ Change that password periodically

(Continued on page 17)

(PASSWORDS—Continued from page 16)

- ✓ *Never reuse* that password at other Web sites
- ✓ *Add Salt* (8 to 12 characters is a good start)
- ✓ And did I mention….You should always use a Password Manager 'cuz your memory ain't that great.

In part 2, titled "The Monkey & the Typewriter," I will teach you how those hash algorithms work, why no one can reverse (un-encrypt, decode, break, crack, hack — call it what you want) a hashed input. And I will even make you smart enough to create an 11-character hash when given a LONG input string. I promise you will never try to reverse a hash again. And I will show you more examples of how the bad guys do their thing to make you *think* they are "cracking" your password.

Let me emphasize this about Password Managers. You should *never* add your salt to the passwords you store *in* your Password Manager. Just store your passwords as normal text. And when you enter it onto a site, then you add your salt. Then if anyone ever gets one or more, or all of your passwords, it will be of no use to them at all. Carry your own salt. Apply when needed.[7]

… TDB

Endnotes, some helpful sites, and additional resources—

[1] Pawned Passwords are 613,584,246 real-world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they are at a much greater risk of being used to take over other accounts. Has *your* password already been compromised? https://haveibeenpwned.com/Passwords

[2] What is Hashing (and how does it work?) https://www.sentinelone.com/cybersecurity-101/hashing/

[3] Learn about the 7 Ways Hackers Steal Your Passwords. This article and Part 2 only cover methods 2 and 5, Spraying and Brute Force. YOU still must protect yourself against other types such as Phishing and Keyloggers, Local Discovery and of course Extortion
https://www.sentinelone.com/blog/7-ways-hackers-steal-your-passwords/

[4] Learn about adding SALT to HASHING from the perspective of those on the inside who create the systems to manage passwords. https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/

[5] A smaller list of 14,344,391 of the most common passwords discovered in various data breaches worldwide (plus some very odd strings!) at https://md5hashonline.com/most-common-passwords where you can see the results of the more than 50 hash functions, plus 115 MD5 variations on each. To search for a specific password or hash string, use a site-specific Google search such as this …
'hello kitty' site:https://md5hashonline.com/most-common-passwords

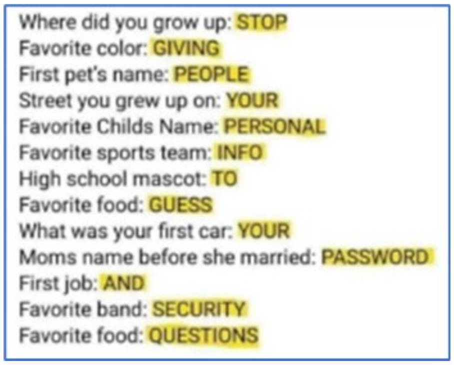
[6] Aren't there actual programs that try to 'crack' a single password? Yes, of course. A popular one is Hashcat. How does it work?
https://www.csoonline.com/article/3542630/hashcat-explained-why-you-might-need-this-password-cracker.html

Additional Resources

A quick evaluation of how secure your password is at
https://howsecureismypassword.net/
A couple easier to use websites that will make hash for you at
SHA-256 https://www.freeformatter.com/sha256-generator.html#ad-output (has a good tutorial)
MD5 and SHA-1 https://www.md5hashgenerator.com/
https://md5hashonline.com/?s=nothing Replace 'nothing' with something else

Don't Let Your Identity be Compromised!

By Jeff Wilkinson, President
Sun City Summerlin Computer Club
https://www.scscc.club
president.scscc (at) gmail.com



Where did you grow up: STOP
Favorite color: GIVING
First pet's name: PEOPLE
Street you grew up on: YOUR
Favorite Childs Name: PERSONAL
Favorite sports team: INFO
High school mascot: TO
Favorite food: GUESS
What was your first car: YOUR
Moms name before she married: PASSWORD
First job: AND
Favorite band: SECURITY
Favorite food: QUESTIONS

We should all be cautious answering those seemingly innocuous questions posted on social media sites such as "*What Year Did You Graduate High School?,*" or "*What City Were You Born in?,*" "*Can You Remember Your Childhood Phone Number*?" or "*Who was Your First-Grade Teacher*?" and on and on. These interesting questions appear harmless and appealing as you develop friendships and reminisce with old and new friends on social media, but beware! Many of these answers can be used to answer or reveal security question answers you chose when you set up accounts at your bank, utility company, etc. For example, when you forget your password, as happens all too often, you will be asked to answer security questions from when you initially set up your account, in most cases some time ago! In addition, answers to these types of questions posted on social media or quizzes can be used to build a profile on you with the information needed to open a new account.

Keeping your identity secure on social media is essential to your financial and personal safety. Unfortunately, identity theft is evolving, with thieves using the latest technology to move from credit card counterfeiting to checking and savings account takeover. A May 2020 study by Javelin Strategy and Research found account takeovers — identity theft where a criminal gains unauthorized access to an online account belonging to somebody else — are trending at the high loss rate, up a staggering 72% over the prior year.

Remember that when you first create a social media account, you provide personal information such as name, age, email address, etc. And I venture to guess that most of us have never read the small print terms of service provided by the host. As you traverse the various pages, forums, postings, etc., data mining creates a profile of your behavior, likes, and dislikes. This information is often monetized by the host sites you visit, meaning sold to third parties. Facebook collects data from all devices you have installed their app on. The language used and time zone can include your device location, data provider, or internet service provider. Data on sites you like or visit via a link on Facebook is also collected.

What can consumers do to protect themselves?

- Keep your software up-to-date.
- Log out of social media sites when finished, particularly when in a public location or using a public computer.
- Use two-factor authentication wherever possible.
- Used strong passwords — keep track of them with a password manager.
- Use a screen lock on portable devices.
- Don't conduct business or share critical information on public Wi-Fi

(Continued on page 7)

About The Dayton Microcomputer Association, Inc. (DMA)

By Peter Hess, DMA President, 2018-2020

About forty-five years ago, a small group of computer enthusiasts from the Dayton, Ohio area gathered around a kitchen table looking at, and playing with, an early personal computer called the Altair 680 that one of them had purchased. This computer had been featured earlier on the cover of the January 1975 issue of *Popular Electronics* magazine. Paul Allen had shown the selfsame article about the Altair to Bill Gates, and later, they wrote software together for that computer. Still later — and still together — Allen and Gates founded the Microsoft Corporation.

Shortly thereafter, those Dayton-area computer enthusiasts joined together with many others to form The Dayton Microcomputer Association (DMA), now one of the oldest (if not *the* oldest) continuously-operating computer user groups in the world. Typically, computer user groups, and the newer iteration, technology user groups, are volunteer-run operations. The DMA is an all-volunteer led, organized, and run 501(c)(3) non-profit organization.

Now, there are hundreds of computer (or technology) user groups in the world, all of which continue to foster improved communication between technological equipment and software publishers, and users of their products. User groups (both computer and technology) provide an environment where more experienced technology users introduce additional and advanced techniques to novices.

DMA offers both monthly General Membership Meetings, which cover new and innovative topics including a wide range of generic technological topics, and its Special Interest Groups (SIGs) which address concerns about specific technology interests. There are eight different SIGs sponsored by the DMA, covering such topics as the Linux operating system, various programming languages such as Python, the use of technology to investigate genealogy, and digital aids to investing. Neither SIG members nor attendees at DMA General Meetings need be members of the parent organization, though they are encouraged to join so DMA can continue providing its services to the public.

Annual dues for DMA membership, which have not been raised for decades, are $25 for Regular Members, and $12.50 for Family/Associate Members (someone living at the same address as a Regular Member). Nonvoting Student Memberships are *free* to students through age 22. Door prizes at General Meetings, picnics, banquets, and other DMA events, and both product and service discounts are available to all DMA members. **... TDB**

Dayton Microcomputer Association Membership Form

Today's date ______/______/__________

□ ***NEW*** Please credit the DMA member who recruited me: ______________________________

□ ***RENEW*** Contact information below is new □ Y □ N

TYPE OF MEMBERSHIP

□ ***REGULAR***

Name ______________________________ Home / Work (_____) _____-__________

Email ______________________________ Mobile Phone (_____) _____-__________

□ ***ASSOCIATE*** Family Associate membership is for a family member living at the same address as a Regular member. Name of Regular member: ______________________________

Name ______________________________ Home / Work (_____) _____-__________

Email ______________________________ Mobile Phone (_____) _____-__________

□ ***STUDENT*** Free Student membership is available to those under 22 years of age, enrolled full-time in a program of higher education. Name of School: ______________________________

Name ______________________________ Home / Work (_____) _____-__________

Email ______________________________ Mobile Phone (_____) _____-__________

Home Address ______________________________

City ______________________________ State ______ Zip __________

INTERCHANGE

Skills & interests you might share with DMA ______________________________

What you hope DMA will provide ______________________________

□ ***SHELL ACCOUNT*** A shell account on the DMA web server provides file storage, hosting of a personal non-commercial website, @dma1.org email alias (forwarding address), all for a one-time fee of $10. A username must be 8 alpha characters. The usual default is last name and first initial, no caps or punctuation. DMA reserves the right of final decision on all usernames: 1st choice ________________ 2nd choice ________________

DUES AND FEES

Regular membership	$25.00 x □ 1yr □ 2yr □ 3yr	$_______
Family Associate membership	$12.50 x □ 1yr □ 2yr □ 3yr	$_______
Student membership	FREE	$ 0.00
One-time setup fee for Shell account	$10.00	$_______
Total		$_______

**Note: $10.00 fee will be charged for any returned checks*

Make your check payable to:
Mail check and application to:

Dayton Microcomputer Association, Inc
PO Box 4005
Dayton OH 45401-4005

Or use Paypal to send your payment to: **membership@dma1.org**

DMA use only

Member# __________ Exp ____/______ [ ] Cash [ ] Check# ________ [ ] Paypal Proc by ________________

Member# __________ Exp ____/______ [ ] Cash [ ] Check# ________ [ ] Paypal Proc by ________________

Member# __________ Exp ____/______ [ ] Cash [ ] Check# ________ [ ] Paypal Proc by ________________

Revised February 25, 2020