

Cyber Bulletin



OCTOBER:2020

CYBERSECURITY
AWARENESS
MONTH



Those Pesky Car Warranty Calls

By Kurt Jefferson, Editor, Central Kentucky Computer Society

Nearly every other day, I receive an obnoxious voice mail: Your car warranty has expired. This is the final call. If you don't respond now, you will get no extended warranty coverage.

Those calls go to my iPhone's voice mail without bothering me because the robocall slayer software known as Nomorobo recognizes this is snake oil and keeps my phone from ringing.

Now, NPR has dissected the calls and given us an inside look at what's really going on.

It turns out if you pay for this service, it covers very little, according to NPR's Planet Money. If you paid a monthly fee, the company claimed to cover your car bumper to bumper. But it turns out the warranty was worth about as much as the paper it was written on. Furthermore, this was all promoted in a very deceptive way, says the NPR article.

(Continued on page 3)

*"Members Helping
Members"
(since 1983)*

Board of Directors

2020-2021

President

Phil Bock

president@lcace.org

Vice President

Linda Busch

vicepresident@lcace.org

Secretary

Bobby Jacobs

secretary@lcace.org

Treasurer

Judy Dunham

treasurer@lcace.org

Programs

Linda Rohlfing

programs@lcace.org

Membership

J.J. Johnson

membership@lcace.org

Public Relations

Linda Koudelka

pr@lcace.org

Volunteers

Webmaster

J. J. Johnson

webmaster@lcace.org

Newsletter Editor

Mike McEnery

editor@lcace.org

Historian

Lester Larkin

historian@lcace.org

Lake County Area Computer Enthusiasts

c/o Group Ambassador

"J.J." Johnson

News Journal

The LCACE News Journal is published eleven times annually. Members are encouraged to submit contributions which will be acknowledged in this newsletter. Send articles to editor@lcace.org. Permission is granted to reproduce any or all parts of this newsletter in other User Group publications, provided that credit is given to LCACE and the individual author (s). Logo designed on an Atari Stacy Laptop in 1989 by Dwight Johnson Jr.

Membership

LCACE membership is open to all individuals and families interested in personal computing. Annual dues are \$20.00 per individual/family. Applications for membership may be obtained at the monthly meeting, by request on the club hotline, and are now available on our web site at <http://www.lcace.org>.

Meetings

LCACE meetings are usually held on Saturdays at the Grayslake Area Public Library, 100 Library Lane, Grayslake, Illinois. The meeting room opens at noon and the formal meeting begins at 12:30 p.m. All meetings are open to the public. Bring a friend!

Newsletter Submissions

Club members are welcome to submit classified ads, reviews, tips and other articles for publication, to our newsletter editor in Microsoft Word format (.doc). **Publication deadline is the 20th of the month for all ads and articles.** Please do not use tabs or special formatting.

Newsletter Advertising

Ad rates per issue: Full page - \$25, Half page - \$15, Quarter page - \$10, Business Card - \$5. Discounts are available on advance purchase of multiple issues. Please send camera-ready copy and payment to the club address by the 15th of the month preceding publication. For more information on ad pricing, please call our Hotline. Ads are **FREE** to all paid members.

Notice

LCACE WILL NOT CONDONE or knowingly participate in copyright infringement of any kind. The *LCACE News Journal* is published by and for LCACE members. Opinions expressed herein are those of the individual authors and do not necessarily reflect the opinion of LCACE, the membership, the board of directors, and/or our advertisers.



(Continued from page 1)

The piece notes the contracts sold were legal. But if you tried to cancel the service, your patience was taxed to the max.

NPR says the standard operating procedure was to force customers to talk to six or seven people to cancel. Then, while speaking to that individual, the company would purposely terminate the phone call. Then the customer had to go back through the process all over again to try and cancel their service.



It turns out despite all this, the company called U.S. Fidelis was doing very well. According to NPR, "One of the owners spent \$26 million building a mansion with a bowling alley and all these secret rooms and this weird walkthrough shower that was kind of like a car wash for your body."

By 2007 or 2008, the complaints began piling up. Since word was getting around that U.S. Fidelis customers were quite unhappy, the company turned to a new way to promote itself: robocalls.

By one estimate, U.S. Fidelis sent out one billion robocalls pitching its product – in just ten months.

As tempers flared and unlucky recipients of these phone calls fumed, more than 40 states began going after U.S. Fidelis and its robocalls. NPR reports U.S. Fidelis was banned from robocalling. In addition, dozens of news articles, TV and radio news reports, and Internet news stories blasted the company. Finally, U.S. Fidelis customers vented during news interviews. They were red hot angry.

Tales of families sitting down for a nice evening supper interrupted by these robocalls surfaced.

Folks who could hardly afford to buy these so-called "extended car warranties" were spending hard-earned

dollars.

Eventually, the company went bankrupt.

So that's the end of the extended car warranty robocalls, right? Not. Exactly.

NPR reports, "It's been ten years since US Fidelis went bankrupt, and now these auto warranty calls are back with a vengeance. But unlike with US Fidelis, many of these calls do not name the company calling you. So, while the federal government tries to figure out who exactly is calling, you will continue to be robocalled and asked about your car's extended warranty."

Read and hear the NPR story [here](#).

More stories:

FCC - [Combating Spoofed Robocalls](#) with Caller ID Authentication

FTC says [hang up](#) on car warranty robocalls

[Car Warranty Scam Robocalls: Here's Why You Get So Many \(And How to Stop Them\)](#)

Tricky Spam Emails

By Jim Cerny, Forums Coordinator / Instructor, Saratoga Technology Users Group

You probably are all aware of those awful spam emails that come to you in your inbox. But recently, I had a very sneaky and tricky spam email that appeared to come from a friend, and I need to tell you about it so you can be very careful.

First, I received a brief email from a friend of mine who was also listed in my contact list, but I found out later that the source email address was not really his. It "looked" like his, even having his wife's first name in it, but it was NOT his email address; it was from a different email provider, which he never used. Yes, that was tricky all right, but later that week, I received one even worse. The email sent to me appeared to come from another friend and, being very careful, I "hovered" my mouse on the email address, and it did show his actual email address, exactly as it is entered in my contact list! But it was NOT from him. Fortunately, I called him, and he confirmed that

(Continued on page 4)

(Continued from page 3)

someone had “stolen” his email address and was using it to try to get gift cards from people.

So, in addition to the usual email precautions, I would like to offer these to help you from being scammed –

+ Brief emails from a “friend” that say something like “Can you help me?” or “Can I ask a favor?” are clues that they are bogus. Call your friend to confirm if they really need your help. As they say, if it was really urgent, they would have called you, not sent an email.

+ If you do reply to such an email by mistake, you will get a follow-up email with a sad story and an urgent request for something like a “cash card” or donation. Don’t do it!

+ Do not reply or provide ANY personal information in ANY email. Emails can be forwarded to anyone anywhere. Valid email addresses are traded like stolen credit card numbers.

+ **Do NOT** send money or credit card information in any email. Instead, use your online banking to pay bills.

+ **THINK** – did the email text really appear to be something your friend would write to you? If there is the least bit of oddness about it, call the person.



How do these scammers get started? Our neighborhood has a directory provided to all residents, which includes phone numbers and email addresses. Many people purposely do not provide their personal information in such a directory. Once you get an email address, I suppose it is possible to tap into some emails sent by that address and thus obtain many more email addresses.

Finally, it appears a scammer can send an email that appears to come from someone else’s address, and yet they still receive replies to the scammer’s email inbox. How they do this, I have no idea, so be careful.

One final story – I was at the Walmart customer service desk when an older man was requesting a money transfer to his son, who needed money quickly. The Walmart people knew right away that it was a scam and refused to fulfill his request. The man was angry, but it was the right thing to do. He wanted to send “his son” several thousand dollars!

The Anatomy of a Scam: Ransom for My Files

By Kurt Jefferson, Editor, Central Kentucky Computer Society

In mid-February, I checked my Gmail account as I do several times a day. Lurking in my Junk folder was a mysterious email message that appeared to come from Germany.

The email address used to send the message might be stolen or forged. But the subject is clear:

Payment for your account.

This is a new form of what’s called “ransomware.” It used to be that criminals would install software on a user’s computer and encrypt all the files – basically locking them so the user can’t read them. The victim would get his or her data back after meeting ransom demands.

Hospitals and other health care facilities have been targeted in recent years, and these attacks have escalated.

Now scammers are sending emails containing ransom demands – even without installing any software.

That is the gist of the email I received in my Gmail account. So, it appeared on both my Macs and iPad.

I'm sharing the message with readers of this newsletter to alert you – should you receive a similar threat.

Payment for your account

Feb. 17, 2021 at 4:33 P.M.

From: webmaster@dreirad*****.de

To: Kurt

Greetings!

I have to share bad news with you. Approximately few months ago I have gained

access to your devices, which you use for internet browsing.

After that, I have started tracking your internet activities.

Here is the sequence of events:

Some time ago I have purchased access to email accounts from hackers (nowadays, it is quite simple to purchase such thing online).

Obviously, I have easily managed to log in to your email account [email account name deleted].

Obviously, I have easily managed to log in to your email account [email account name deleted].

One week later, I have already installed a Trojan virus to Operating Systems of all the devices that you use to access your email.

In fact, it was not really hard at all (since you were following the links from your inbox emails). All ingenious is simple. =)

This software provides me with access to all the controllers of your devices (e.g., your microphone, video camera and keyboard).



I have downloaded all your information, data, photos, web browsing history to my servers.

I have access to all your messengers, social networks, emails, chat history and contacts list.

My virus continuously refreshes the signatures (it is driver-based), and hence remains invisible for antivirus software.

Likewise, I guess by now you understand why I have stayed undetected until this letter...

While gathering information about you, I have discovered that you are a big fan of adult websites.

You really love visiting porn websites and watching exciting videos, while enduring an enormous amount of pleasure.

Well, I have managed to record a number of your dirty scenes and montaged a few videos...

If you have doubts, I can make a few clicks of my mouse and all your videos will be shared to your friends, colleagues and relatives.

I have also no issue at all to make them available for public access.

I guess, you really don't want that to happen, considering the specificity of the videos you like to watch, (you perfectly know what I mean) it will cause a true

catastrophe for you.

Let's settle it this way:

You transfer \$950 USD to me (in bitcoin equivalent according to the exchange rate at the moment of funds transfer), and once the transfer is received, I will delete all this dirty stuff right away.

After that we will forget about each other. I also promise to deactivate and delete all the harmful software from your devices. Trust me, I keep my word.

This is a fair deal and the price is quite low, considering that I have been checking out your profile and traffic for some time by now.

In case, if you don't know how to purchase and transfer the bitcoins - you can use any modern search engine.

Here is my bitcoin wallet: (Bitcoin wallet deleted)

You have less than 48 hours from the moment you opened this email (precisely 2 days).

Things you need to avoid from doing:

*Do not reply me (I have created this email inside your inbox and generated the return address).

*Do not try to contact police and other security services. In addition, forget about telling this to your friends. If I discover that (as you can see, it is really not so hard, considering that I control all your systems) - your video will be shared to public right away.

*Don't try to find me – it is absolutely pointless. All the cryptocurrency transactions are anonymous.

*Don't try to reinstall the OS on your devices or throw them away. It is pointless as well, since all the videos have already been saved at remote servers.

Things you don't need to worry about:

- That I won't be able to receive your funds transfer.
- Don't worry, I will see it right away, once you complete the transfer, since I continuously track all your activities (my trojan virus has got a remote-control feature, something like TeamViewer).
- That I will share your videos anyway after you complete the funds transfer.
- Trust me, I have no point to continue creating troubles in your life. If I really wanted that, I would do it long time ago!

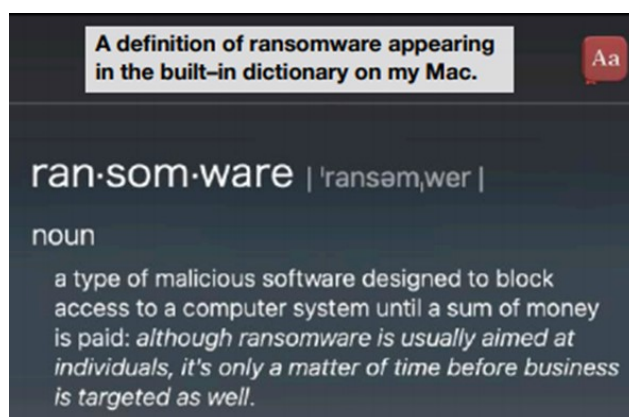
Everything will be done in a fair manner!

One more thing... Don't get caught in similar kind of situations anymore in future!

My advice - keep changing all your passwords on a frequent basis

So there you have it. Obviously, I'm not about to pay a ransom. And my files have not been locked.

Hucksters are sending out these emails worldwide, hoping someone will be terrified and meet their demands. It makes the Nigerian email scams and pleas for help via email (please send money now – John or Mary has been hurt while visiting London or Paris or Sydney or Madrid or...) seem rather tame, doesn't it?



Don't Respond to Potential Scams

By Dan Douglas, President, Space Coast PCUG, FL

PLEASE PRINT THIS OUT AND PASTE IT NEAR YOUR PC AND READ IT BEFORE RESPONDING TO ANY POTENTIAL SCAMS.

Unfortunately, I have seen a dramatic increase in people seeking help after being scammed on their computers. Unfortunately, this includes some of our SCPCUG members. So, this month, I would like to share some precautions you can take to minimize your exposure to getting scammed on your computer.

Let's look at the most common ways of enticing people to fall for these schemes:

1) Phone Calls - Receiving or placing a phone call, supposedly from or to some recognizable, well-known/trusted organization, such as Microsoft, Dell, Amazon, HP, etc.

Prevention and best practices to avoid falling victim:

If you want to contact an organization, go to their official website and click on the contact us link. Do not search for contact info. Scammers pay to be listed first on common searches and will act as if you are calling the real company. I've seen this many times with people trying to call HP for printer issues or supplies. They do a web search and call the first number that comes up, and the person convinces the caller that their printer may need an update, and if they give them remote access, they can check it out, and then it is game over.

It is extremely unlikely you would ever receive a phone call regarding your PC or any activities you perform.

My advice is to immediately hang up on anyone claiming to be calling from one of these organizations.



2) PC Messages - Receiving a screen message on your PC that informs you - take your choice - you have been hacked, you are in danger of losing your banking passwords, your PC has been used for illegal acts and will be reported to the FBI, your IP address has been traced, etc. The message usually states to not turn off your PC and to call some number immediately.

These are commonly delivered through your browser (Edge, Chrome, Firefox, etc.) but can be cleverly designed to hide where it originated from or look exactly like common company messages by using their logos and copies sections from their actual web pages.

Prevention and best practices to avoid falling victim:

Ignore the message – do not be scared or worried. Instead, immediately force your computer to shut down completely (NOT sleep) – pull the plug if you need to. The scammer will usually disable many of the common ways to close the program/browser normally, such as preventing

(Continued on page 8)

(Continued from page 7)

you from clicking on the close X in the top right-hand corner, so forcing the power off may be the only way. Usually, the scam will not permanently infect, corrupt, or access any of your information if you shut it off immediately. Download the free version of Malwarebytes from www.malwarebytes.org if you want to be sure all traces are removed. If you let the scammer have remote access to your PC, you may need to change your accounts (credit cards and financial) and their passwords to be safe.

3) Email – Opening an attachment or clicking on a link embedded within an email can launch any one of many forms of 'attacks.'

Prevention and best practices to avoid falling victim:

The first thing that I always do when I get an email that may be suspicious is to check the sender's email address. Your email program may always show this address, or you may need to hold the mouse over the name to see the actual email address that was used to send the email. Anything that doesn't look normal, such as a domain name that is not the same as the company name, or a sender ID that looks made up, such as `dsae12345@myname.com`, I would delete/flag that email as junk and report it as a phishing email. Phishing is where the scammer tries to get you to log on to a website that looks like a legitimate one but really captures your login information – common ones are banks, PayPal, and Amazon. Never open an attachment without checking the sender's email address first. Malwarebytes is a good program that may be able to block many scam programs before they are active if you are using the premium version.



I Was a Fool, So You Don't Have to Be

By David Kretchmar, Hardware Technician
Sun City Summerlin Computer Club

I don't necessarily think of myself as a fool, but I did a foolish thing a few years ago. I bit on one of Motley Fools' ubiquitous teaser internet ads promoting the best new emerging technology stocks that were about to "explode." I paid (I think) \$29 to Motley Fool to get the names of the stocks. Motley Fool sent me the names of several mostly small and pink sheet stocks. Most pink sheet companies are highly speculative, have little or no earnings, and are low-priced penny stocks. For many pink sheet stocks, a price appreciation up to one penny would be wildly profitable, but well over 90% of these stocks appeared worthless.

I wonder if they are buying shares before they recommend them and running the shares up and then maybe even shorting them or just taking advantage of people willing to pay for their information. Their expertise seems to be selling themselves, not researching companies.

The Motley Fool's website is self-described as "A wide-ranging investment resource that intended to educate, enrich, and amuse individual investors around the world." The site includes discussion boards, quotes, data, and of course, stock-picking advice. Many of the articles are voluntarily contributed by various individuals. Unfortunately, I suspect that

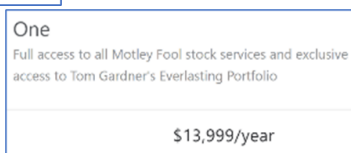
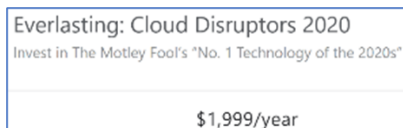
(Continued on page 9)



many have taken a position in the stocks they are now pumping, not unlike the Motley Fools, with hopes of profitable dumping.

Upsells

If you are not satisfied with the advice provided according to your original subscription, the Motley Fools will offer you "better" subscriptions, such as:
Or



A Foolish Website

I am not new to the stock market; I focused on security analysis in college and have been doing my own research for over 50 years. Almost everything I have seen from the Motley Fools is absolute garbage. I



highly recommend not using their website for any information except maybe for the entertainment value of how foolish it is. Often there are contradicting opinions on the same stock on the same day!

There is way too much advertising on the Motley Fools subscription website. This site is without transparency and, therefore, of questionable value for investors. Suppose you want to be successful, and actually be one of the rare investors who make money relying on the advice of others. In that case, you need to receive information from people whose own investing/trading results you can clearly see. There are several dozen articles every day, and I believe no one could construct a good trading strategy based on the hundreds of stocks they say are "ready to explode."

The Motley Fool's subscription website is a mess of marketing. Most of the articles provide virtually no actionable information, except pitches for more expensive Motley Fool newsletters. Occasionally there is a well-written article that contains decent information, but this is rare.

To be fair, I do agree with their philosophy that a

buy and hold strategy, not trading, is the path to real wealth accumulation. They deride ALL short-term trading dogmatically but make tons of picks, some work, others totally fail. Also, they advise not to both-er trying to time the market; just spend time in the market holding your winners and trimming losers. So there – in this paragraph, I've reflected virtually all of the sound advice you are likely to glean from the Motley Fool website – and it was FREE!

Can they do 5X better than the market?

It is inconceivable that The Motley Fool could beat the S&P 500 by over 500%, as they claim in their current advertising. Most professional money managers and advisors have difficulty equaling the performance of the market averages. Those who are considered investment geniuses, such as Peter Lynch and Warren Buffett, could beat the market by a few percentage points a year. Anyone able to beat the market averages by 500% would be able to amass great wealth investing and would not have to sell a tout service.

Even the free offers are less than worthless

Almost every day, I see Motley Fool teaser articles on sites such as Yahoo Finance, and often the headline is misleading. The article provides just a superficial discussion of a stock. Usually, the article ends stating the stock discussed is OK (or bad), but the Motley Fools knows ten stocks that are better, which they will provide to you if you just furnish your email address. I have done this several times (providing my "junk" email address) and have never received the information the Motley Fools promised. Instead, they bombard my mail account with worthless spam. I suspect they also sold my email address since I also started receiving spam from unknown companies.

The sports betting scam

When I worked as a Special Agent in a former life, I was involved in investigating an off-shore sports betting site. The owners of this site quickly discovered they could make more money selling gambling advice, also known as tout services, than from the bets themselves. The profit on sports bets was about 5 percent – (10% of losing bets), similar to on-shore bookies and casino sportsbooks.



(Continued on page 10)

(Continued from page 9)

Say Boston was playing New York, they would tell half their new subscribers (or potential subscribers) to bet on Boston, and the other half New York. After the game, half of their customers would feel their handicapping might be good, and the other half would probably quit. The subscribers who stayed would tell half of them to bet one side of a game and the other half to bet the other side. Again, half of their customers would think they were great, and the other half would have their doubts. After doing this once or twice again, they would have a smaller pool of customers who thought they were geniuses and would pay big bucks for their next tip.

Conclusion

The Motley Fool and many other stock picking services operate similarly to the sports tout scam. But, at least they are no fools; only people who buy their services are.

A Monkey and a Typewriter Make a Hash with Shakespeare and a Soccer Ball

By Arthur Gresham, Editor, UCHUG Drive Light

Under the Computer Hood User Group

www.uchug.org

Passwords and Hash, Part 2

This discussion is a follow-up to Part 1 **PASS(word) The Beef, the Hash, the Salt for Einstein, and Dictionary**, in which I introduced the process hashing passwords and the concept of Salt.



a
of

During a continuing discussion with a friend, while writing part 1, I finally realized that we were looking at the same things and coming to different conclusions regarding passwords. For example, we debated whether passwords stored as a hash code are really easy to un-encrypt (decode/crack/break/hack) or really hard.

We Both Win

It turns out we are all using the wrong terms. Yes, the hash code for a short password is of little value because it can be determined quickly. He wins. But it is also a fact that a hash code cannot be un-encrypted. I win. I will demonstrate both of these concepts in this article.

The big problem is because several terms are being incorrectly used for the world of hashing and passwords. Let me explain by using very simple examples from our shared experience.

The Gorilla in the Room

You may recall a theoretical discussion when you were in school. Something about a monkey in a room with a typewriter being able to write the works of Shakespeare if he has enough time to randomly peck the keys. This thought experiment is called the **Infinite monkey theorem** (read about it [in Wikipedia](#) (1) if you have forgotten how it works).



The strings produced by Hash Algorithms look like something you might think was written by that monkey. We expect that most of what that monkey typed is gibberish. Likewise, the hash for a particular input text (or a picture or an entire operating system, library, or simple password) is an 'indicator'. This text appears to be pure gibberish. That is because it does not contain anything actually from the input. The key here is 'contain.'

The Key is the Container



Let me illustrate that in a different way. You are all familiar with ZIP or RAR, or other compression functions. You have undoubtedly downloaded some program, text, spreadsheet, or audio file, which was sent to you

(Continued on page 11)

(Continued from page 10)

as a compressed file. When you get the file, you 'unzip' it into a folder, then read, watch, listen to, or somehow use the contents inside that file. The zip was much smaller than the original contents inside of it. Yet, it contains an EXACT duplicate of the original inputs. If it didn't, you would be very upset. Your program would not run, or your audio would not play, or the words in the text would turn into uwwka08qkj k3lksd fjasdhd rhandnt making you very confused and unhappy. This is a two-way process, In and out.

Hash Algorithms are not a zip of the original input. While the Zip file was easy to unzip because it is designed as a two-way process, the Hash is a one-way process. You can MAKE a hash, but you can't UN-MAKE it. It does not 'contain' any information about the input string; it cannot be cracked. Again, this is a one-way process. What goes in can not come out.

As an extreme example, this week, I installed a new version of Linux on the computer I am typing on right now. The download was a 2 Gigabyte file. Part of the install instructions are to compare the SHA-256 Hash (2) of this download with a given 256-byte check value. The SHA-256 Hash from the authorized site must match your value to ensure that yours is a complete, unaltered download. But the SHA-256 Hash does not contain all of Linux Mint 20.2 Cinnamon and all its files. If it did, I could have just downloaded the Hash, UN-MAKE it, and installed it. So, the files aren't contained in the Hash.

Yet if I create the SHA Hash for the string 'A' (that is just the letter A), I will still get a 256-byte hash value. And it certainly does not compare to the contents of my Linux download.

This is because a Hash is only what is called an 'indicator' value.

The Container has a Key

Let me give you another example and use a couple of other terms that have been misused in this discussion. Perhaps you remember WW 2 (No, I am not trying to age check you, so put your hearing aids back in



your ears and listen up). During the war, the radio became a vital tool for communications. The allies used it to communicate from London to the generals in the field. But they did not simply use plain words to give instructions. Instead, those instructions were processed with machines that scrambled the letters. The messages were 'encrypted.' Headquarters used a KEYCODE to garble the text. That text was sent by radio, and anyone with a receiver could get it. But only our side (mostly) had the matching KEYCODE to UN-Encrypt the message.

With our fast, modern-day computers, perhaps we could now DECODE or CRACK those messages (simple cipher codes), but they did not have the means to do it then, so the messages were secure.

But here again, the messages were designed as Two-way messages, containing the plain text going in and coming out with the same exact text when un-encrypted. If it wasn't exact, it would have been of no use in the war effort.

With Hash Algorithms, there is no Container. There is no KEY. No Unzipping. No Coding-No De-Coding, No Encryption-No Un-Encryption. Because a Hash is only an 'indicator' value.

Time to make Hash

Time for some fun. I want to program you brain. I want you to be my Hash Function Computer. You will have only one job. That is to give me an answer to the question I will ask. Trust me, you have the brain-power to do this.

Here is your input text:

I am larger than a softball, smaller than a basketball, I am covered with black and white pentagon shapes, and if you kick me into the net, you will score one point What Am I?

Hint: don't Google it. You will not find the answer...

Just think...

Don't peek...

(Continued on page 12)



Time is Money

Got your answer?

Did you make hash?

If you said "soccer ball," you are right. Those 11 characters are the hash of that input string. I told you this was easy. BUT if I had said to you "soccer ball" at the beginning of this article or in a conversation, what is the chance you would have responded with the exact text -

"I am larger than a softball, smaller than a basketball I am covered with black and white pentagon shapes, and if you kick me into the net, you will score one point What Am I?"

But wait. There are many Hash Algorithms and what you just gave me was the American-11 algorithm. What would you have said if you lived in London?

Sure, I hope you understand in that part of the world, they have said FOOTBALL .

Because that, you see, is the British-8 algorithm. Not to be confused with the Spanish-6 algorithm, which would have said FÚTBOL . Different Algorithms might produce different lengths. Yet, they are all only 'indicators' of the same exact input. But they do not un-anything any of them. The hash does not contain the input string. So it can't be Cracked.

A Hard Nut to Crack?

In the paragraph titled We Both Win, I said, "the hash code for a short password is of little value because it can be determined quite easily."



While a short input text of a hash code may be determined quite easily, note that I did not say it could be Un-Encrypted or Cracked. For this demonstration, I will be using the Art-4 algorithm. Thus, any input string will generate a 4-character hash (cuz my brain is very small).

You will be playing the part of the internet's bad guys. First, I will show you five input strings (a dictionary of passwords) that have been hashed with the Art4() algorithm. This will represent the bad guys' precomputed Hash Table Dictionary (see part 1 for a description of this).

Input String ART4() hash

AAAAAAAA = aee9

longword = 9546

Password = dc647

Password99 = e6ab

Willam1 = b4b9

{Note all of these passwords have been [Pawnd](#) (3). Someone has actually used them!}

Imagine a bank had a Data Breach (someone inside opened an email and clicked on a "Link." You know the rest of the story!) The bank had saved customers' passwords using my algorithm. Their records are in the database, which was stolen from a bank.

I want YOU to see if you can 'Crack' any of the bank's data and tell me whose password you 'cracked.'

Here is a bit of the data breach file:

Username	Password hash	Balance
Joe	3255	\$10,100
Mary	7bb4	\$101,000
Beavis 9546		\$52.14
Bill	5835	\$250,000

(Continued on page 13)

(Continued from page 12)

(It takes time, but the lookup yields results, look carefully)

So, did you 'Crack' any of the hash values in the bank database? Could you try to log in with the password of any of these victims?

It looks like user Bevis may lose his savings. Maybe his *longword* just was not long enough. But did you actually 'Decrypt,' 'Decode,' 'Crack,' 'Hack,' or 'reverse engineer' any of the passwords?

NO. You simply found a value that matches a known hash (you found it in your Hash Table Dictionary), and you 'Guessed' what one of the passwords might be. And you would be exactly correct because, as we learned from Einstein in part 1: "we expect to get the same results for a given string every time. To get anything different would be crazy."

By the way, customer Bill, whose root password is William1, will not be in trouble because he salted his password. So, unless you bad guys hash his actual password ("William1") plus his salt (which is "PlusPepper") to get an ART4() hash of 5835, you will not be getting into his account.

And because the bank did not SALT the customer's passwords, a plain language hash dictionary leaves many customers vulnerable for this look-up solution.

Do not let that be you. Use Good Passwords, not common short words or expressions that will be found in the dictionary. And when you do enter or change your password, use SALT if it's valuable, SALT it.



"Don't be a Beavis. Use strong passwords."

"Yeah, Dude...
and Salt it."

Photo Credits

"Picture on Early Office Museum" Author: New York Zoological Society, 1907 Public Domain

"Infinite Monkeys 2008" by Simon Greig Photo is licensed under CC BY-NC-SA 2

"Glass food storage container with Easy Find Lids" by Rubbermaid Products is licensed under CC BY 2.0

"U-505 Enigma Machine (View 4)" by derekbruff is licensed under CC BY-NC 2.0

"hourglass" by secubie is licensed under CC BY-NC-SA 2.0

"Walnut in nutcracker" by wuestenigel is licensed under CC BY 2.0

"Infinite Monkeys 2008" by Simon Greig Photo is licensed under CC BY-NC-SA

"Beavis and Butt-head titlecard" fair use by https://en.wikipedia.org/wiki/File:Beavis_and_Butt-head_titlecard.png#filelinks

[CC](#) creative commons licensed

References

Infinite monkey theorem [Wikipedia](https://en.wikipedia.org/wiki/Infinite_monkey_theorem) article https://en.wikipedia.org/wiki/Infinite_monkey_theorem

SHA-256 <https://www.freeformatter.com/sha256-generator.html#ad-output> has a good tutorial

Pawned Passwords are a dictionary of 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>

A Monkey and a Typewriter Make a Hash with Shakespeare and a Soccer Ball by Arthur Gresham is li-

censed under a [Creative Commons Attribution-ShareAlike 4.0 International License](#).

As long as you attribute this article, you can use it in part, or whole, for your newsletter, website, or blog.



Don't Let Your Identity be Compromised!

By Jeff Wilkinson, President
Sun City Summerlin Computer Club

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*

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**

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. Unfor-

tunately, 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 percent 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 the consumer 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

(Continued on page 15)

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
- 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 [Medicare's fraud office](#) and tax identity theft to the [IRS](#).

It should be clear that you want to avoid this, so a little awareness and preventative steps can help prevent potentially serious problems.

It's Called Clickbait, and You Need to Learn to Avoid It

By Kurt Jefferson, Editor, Central Kentucky Computer Society

I was eating yogurt as I was reading stories about one growing danger on the Web: Clickbait. What I read made me pause and put down my spoon.

It turns out that plenty of us are clicking on email links or Facebook postings sent to us from unknown senders. Unfortunately, this can lead to malware and trojan horses infecting your computer.

The practice is called clickbait. Someone you don't know sends you an email or a Facebook posting. It contains a link. You click on it.

Catchy and provocative headlines are usually a dead giveaway that you're being targeted by clickbait.

Clickbait often contains these qualities:

- Headlines that appeal to your strong emotions, such as humor or outrage
- Headlines designed to grab your attention, leaving you wanting more information
- Headlines that tell you nothing about the content of the article
- The headline is too good to be true
- Content that encourages you to share the item with someone else on Facebook



- Funny images or video

Examples of clickbait headlines include:

**87-Year-Old Trainer Shares
Secrets to Losing Weight**

**When You Read These Shocking
Food Facts, You'll Never Want to Eat
Again**

(Continued from page 15)

Stop Eating Chicken Breasts Immediately

Here's the scary part. A study of 7,804 students by the Stamford Historian Education Group revealed that more than 80 percent of middle school students believed an ad was an actual news story. This, despite the fact that the ad was clearly marked with the words, "sponsored content."

The point is to teach people to recognize clickbait and to avoid it. It's not worth your time.

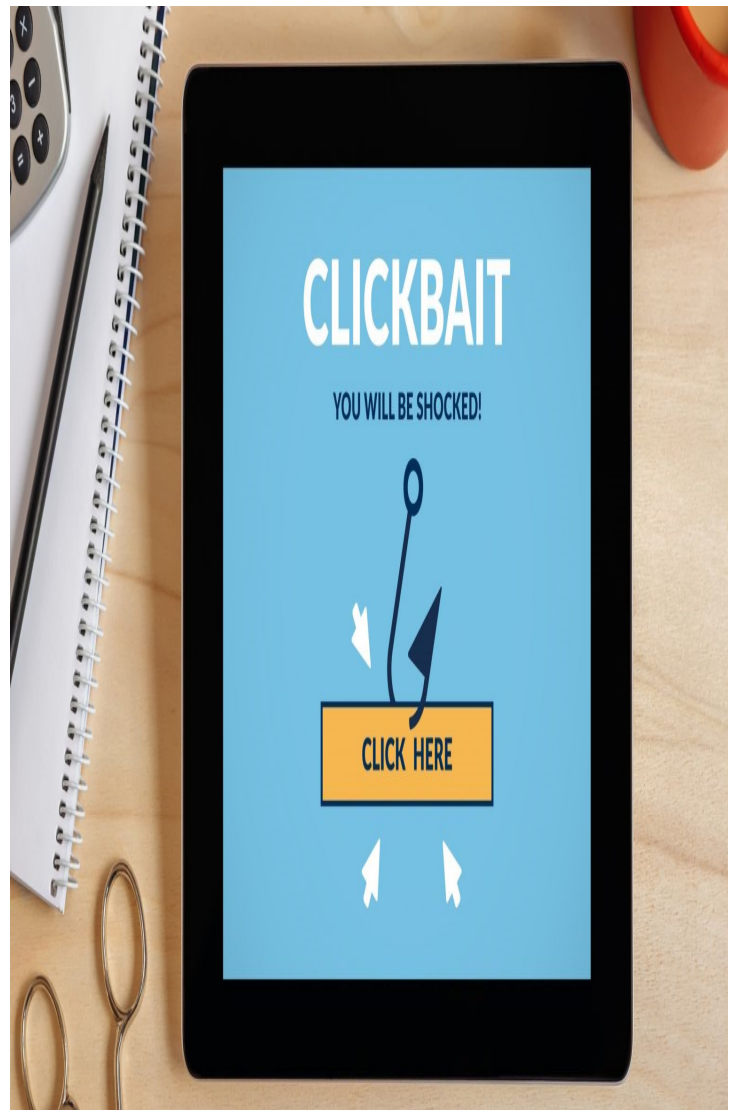
Free IQ tests and credit score checks often ask you to fill in personal information. Unfortunately, you don't know that the website collects your personal details to build a profile on you. Once you submit this information, you'll be subjected to scams and even more links to dangerous websites.

Clickbait links open the door to more spam and potential malware, adware, spyware, viruses, worms, trojan horses, and the real possibility that someone could take over control of your computer. Just say no by refusing to click on links you aren't sure about.

The DealDash (Penny Auction) Scam

By David Kretchmar, Computer Technician
Sun City Summerlin Computer Club

If you watch much TV or surf the internet, you've seen ads promising products as much as 95 percent off retail at DealDash.com or other penny auction sites. DealDash advertises itself as offering fair and honest auctions, but is it really? Millions of people have signed up for a chance to buy items at penny auctions at a fraction of the retail price. Who wouldn't want to buy a new iPad for \$30? But think about it; who would want to sell that iPad for \$30 when it cost several hundred dollars wholesale? It is worth noting that the "penny" in penny auctions refers to the bid increments, but your actual cost could be many dollars.



Consumers are buying more items online every year and appreciate the convenience, selection, and often substantial cost savings. So, these penny auctions would appear to be an extension of that money-saving online buying concept.

Most consumers are familiar with online auctions at sites such as eBay, where interested individuals bid up the price of an item until time expires. The high bidder at the end of the auction wins the item at the winning bid price.

However, another form of online auctions, internet penny auctions, has expanded in recent years. While some of these sites are *technically* legitimate, many of their business practices are questionable, and most consumers would be better off avoiding them altogether.

(Continued on page 17)

How penny auctions work



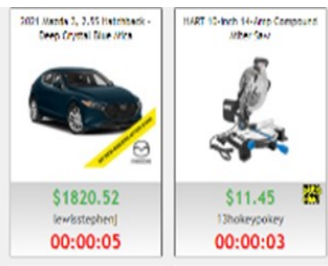
In some ways, online penny auctions are internet bidding sites that share some similarities with legitimate auction sites like eBay. However, the BIG difference is that consumers who

bid on penny auctions must pay for each bid they make regardless of whether they win or lose the auction.

Generally, anyone interested in bidding in a penny auction must pay a registration fee before gaining access to bidding. While not required by all penny auction websites, this fee is often described and charged in what many consider an underhanded way. For example, it is typical for a consumer to make a query regarding online penny auctions. If the consumer provides credit card information, that credit card is immediately charged \$60 - \$99 as part of the registration process. Often consumers provide credit card information without realizing they are authorizing any payment.

An Auction Example

As stated above, penny auctions' business model immediately charges anyone furnishing them a credit card number of at least \$60, which buys 100 bids.



Most new bidders bid on one or two auctions, lose their 100 bids (\$60), and

quickly realize getting a bargain wasn't as easy as it looked. These sites count on the addictive nature of *almost* winning an auction, maybe losing by a penny or two, to encourage a percentage of bidders to buy more bids. Sometimes a substantial discount is offered - i.e., if you sign up right now, you can get 200 bids for the same \$60.

Penny auctions usually allow losing bidders to apply at least part of the money spent on bidding towards buying the product at *their* retail price. However, penny auction sites, including DealDash, often substantially overstate the retail price of items, so buyers are usually either overpaying or perhaps getting completely ripped off.

How the Auction Works

The bidding for an item typically begins at \$0 and then increases by one cent each time someone

bids. There is a countdown clock that restarts every time someone places a new bid. Some websites even allow users to set up automatic rebids if they are outbid. The total price of the item "won" is determined by the number of bids, so you could end up paying well over the retail value of the item you're bidding on. Generally, you have also lost the money spent on the used bids if you lose the bid.

Let's say the auction is for a new computer with a stated retail value of \$599. The bidding starts at \$0, increases in 1 cent increments, and one "lucky" bidder "wins" the computer for \$30. The winning bidder is given credit for the bids he has "spent" at \$0.60 each. It is not unusual to see individuals bidding hundreds of times, so if the winner in this example bid 300 times, that winner paid \$180 for their 300 bids, if each bid cost \$0.60. Still, this does not seem like a bad deal for the winner; \$180 for a \$599 computer, even if it is a system, you could get on Amazon for \$399.

If a penny auction item sells for \$180, the auction site has received 18000 incremental 1 cent bids, which cost the bidders as much as \$10,800! Penny auction sites often promote themselves as "social media" buying and stress the social nature of their sites. What they don't advertise is how addicting these sites can be. \$10 gift cards can go for over \$20 when bidders' egos apparently overrule all common sense. And I can virtually guarantee that YOU will not get that computer for \$180.

An individual cannot determine which penny auction sites are "legitimate." Some state attorney generals have found that some penny auction websites use "shills" that automatically outbid people, making it virtually impossible to win items at a reasonable price. Some of these shills are software programs that show a fake username to persuade consumers that they are bidding against a real person. As a result, several penny auction sites have disappeared, never shipping items won. Other sites have sold financial information about users or put additional charges on credit cards without permission.

Conclusion and Recommendation: Avoid Penny Auctions

While online penny auctions may sound like an attractive deal at first, consumers should be very wary before handing over any money or credit card information. It is doubtful that consumers will save any money by using the service to purchase goods, and much more probable they will be ripped off.

Don't Let Your Identity be Compromised!

By Jeff Wilkinson

President Sun City Summerlin Computer Club

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

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**

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 percent 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 the consumer 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
- Put a credit freeze on your accounts with credit bureaus. [Equifax](#), [Experian](#), [Innovis](#), [TransUnion](#)

(Continued on page 19)



(Continued from page 18)

- 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 [Medicare's fraud office](#) and tax identity theft to the [IRS](#).

It should be clear that you want to avoid this, so a little awareness and preventative steps can help prevent potentially serious problems.

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



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.



Photo 1

Discussion after the presentations moved into questions concerning the passwords we use on all the sites and services on the internet. Several questions and opinions were shared about managing our passwords, how to build passwords, security of passwords, and the impact of losses from the frequent Data Breaches from small and large businesses, government, and anyone operating a website using Password technologies having sensitive information stolen.

The Beef



Photo 2

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 password, or many passwords in a system database. 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 mathematical methods. As a result, there are a lot of myths and misconceptions about



Photo 3

(Continued on page 20)

(Continued from page 19)

how passwords are stored by a corporation (or website) and how one could go about getting a password (and in particular, YOUR password) from that collection of thousands.

For example, how can it be Cracked? Or Hacked? Or UnEncrypted?

The Banker

But let's go back to basics in time a little bit. To the good old days when taking your money to the bank was a face-to-face activity. You walked up to the teller (remember when they had live people doing that?) and handed them your bank passbook.

You gave them your money.

They opened up a big ledger book, turned a few pages, and wrote your deposit into your account.

How did they know what account to credit the money into? Answer: They looked at 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 = Account # written in the passbook (physical possession)

Your Password (only you have it) = 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 ledger book. Instead, your valuable information, pictures, account balance, or credit card number are all stored as ones and zeros on a computer somewhere.



Photo 4

Typically, most of this information is organized in huge databases 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 website, that password

isn't stored verbatim on the website's server. That's because your password could be published and made freely available (Pawnd (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 database record to access YOUR account will now have:

1. Your USER ID = this could be your email address or other name you use as the first entry in your login
2. Your HASHED Password = you must enter a password to verify that they match
3. Your name or other info, which may be encrypted, or plain text
4. Your account number or other internal ID of your account
5. Other data about your account, such as answers to your security questions, preference settings you have made, or any of the other many things about you that set up your use of that online space.

The Hash

More than 50 Hash functions are MD5, SHA-1, SHA-2, SHA-256, NTLM, and LANMAN. (6)

"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.'"



Photo 5

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 they are not compression functions such as ZIP files that errorlessly retain all the original content. I will discuss this in detail in Part 2.]

If a website 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

(Continued on page 21)

(Continued from page 20)

your password. A common hash function 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:

1. **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.

2. **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.

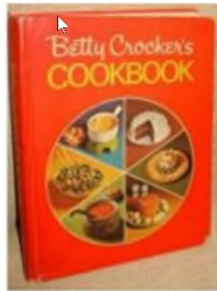


Photo 6

3. **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)

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.

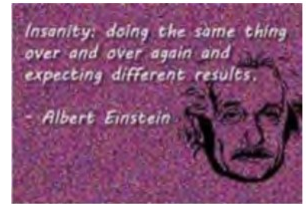


Photo 7

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 their username, 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 database.

Step 3 – Later, when a user logs in, they enter their password.

Step 4 – That entered password is run through the same hashing function as was used before.

(Continued on page 22)



"I think we're named after computer passwords."

(Continued from page 21)

Step 5 – The server checks this hash against the one stored for the user in the database.

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.



Photo 8

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 in a database (this becomes their Dictionary). SO, they can save the hash for all the passwords like '12345' 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 their 'dictionary.' When they look for 'fc5e....' in the stolen database, 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 they 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 database. Just one problem, and it is a big problem; 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 pass-

words (6). For example, Google for ['hello kitty' site:https://md5hashonline.com/most-common-passwords/](#) 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. So, for example, for passwords with just 9 lower case letters (abcdefghi), the number of passwords that could be formed 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 database they have to hash to complete their dictionary. So even if they had a database with all the possible combinations of 9 lower case and 3 uppercase letters, they would have almost 4 x 1020 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 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. They still need the time and disk space for the SHA-1, SHA-256, NTLM, and LANMAN. 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 (7) about Hashcat). It is possible, but.....?)

To Improve the Hash, Add Salt

So, you see the problem here. Einstein told us. 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.



Photo 9

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

(Continued on page 23)

(Continued from page 22)

not, then you should.

Let the cook add the salt.

In this case, the 'cook' is the guy in the IT shop who wrote the routines that are hashing 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 they 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 the cook adds the same salt to every word when they hash it. Thus, more time is added, delaying their access, and costing them 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 hacker's day because they must re-hash every standard password with every salt. That is 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 they 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 (5) 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.

Also, if you use a short-length Master password 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?' they 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 would 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).

SO, here are 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
- **Never reuse** that password on other websites
- **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



Photo 10

(Continued on page 24)

(Continued from page 23)

'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.

Some helpful sites-footnotes and additional resources

- (1) Pwned 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) (2) What is Hashing (and how does it work?) <https://www.sentinelone.com/cybersecurity-101/hashing/>
- (3) (3) Extensive quotes at the beginning of this article are from <https://thycotic.com/company/blog/2020/05/07/how-do-passwords-work/>
- (4) By [Barbara Hoffman](#) May 7, 2020
- (5) (4) 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/>
- (6) (5) 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-tohashing-a-better-way-to-store-passwords/>

- (6) 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/](https://md5hashonline.com/most-common-passwords/)

- (7) 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-thispassword-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](https://www.freeformatter.com/sha256-generator.html#ad-output) (has a good tutorial)

[MD5 and SHA-1 https://www.md5hashgenerator.com/](https://www.md5hashgenerator.com/)

<https://md5hashonline.com/?s=nothing> Replace 'nothing' with something else

Photo Credits

1. "HashandSaltandDictionary" by Arthur Gresham is licensed under CC BY-SA 2.0
2. "Corned Beef and Hash" by gozamos is licensed under CC BY-SA 2.0
3. "Freedmen's bank passbook" by Allen Gathman is licensed under CC BY-NC-SA
4. "Geordi & Data" by JD Hancock is licensed under CC BY 2.0
5. 5. "Red Flannel Hash (9)" by Joelk75 is licensed under CC BY 2.0
6. 6. "Betty Crocker's Cookbook" by Patrick Q is licensed under CC BY-NC 2.0
7. "Insanity by Albert Einstein" by Mimsen is licensed under CC BY-SA 2.0
8. "dictionary-1 copy.jpg" by TexasT's is licensed under CC BY-NC-ND 2.0
9. "salt shaker" by TooFarNorth is licensed under CC

(Continued on page 25)

(Continued from page 24)

BY-NC-SA 2.0 1

13. "Day 76 of 365: kuchenne rewolucje" by Arek Olek (cropped) is licensed under CC BY 2.0

This work by Arthur Gresham is licensed under a [Creative Commons Attribution 4.0 International License](#).

As long as you attribute this article, you can use it in part, or whole, for your newsletter, website, or

blog.

All photos and images are licensed as noted in the Credits under a Creative Commons Attribution 2.0 International License.

Creative Commons Attribution 2.0 International License. Creative Commons Attribution 2.0 International License.



Cautionary Tale about Free VPNs

By Joel Ewing, President, Bella Vista Computer Club

One of the caveats in the VPN article in the March 2021 Bits & Bytes, also mentioned at the March General Meeting, was that free VPN services were not recommended. As if on cue, see the following article recently published by Malwarebytes Labs on "21 million free VPN users' data exposed."

A hack of several free VPN services revealed that not only were some services collecting user activity logs in contradiction of their advertised policy, but some were also collecting email addresses, passwords that were not encrypted, IP addresses, mobile device models, and IDs.

The whole point of using a VPN with mobile devices is to avoid exposing non-encrypted data when using a public Wi-Fi network; but if that data would have been non-encrypted on a public Wi-Fi without VPN, then with a VPN service, it is still exposed non-encrypted within the server of your remote VPN service. In addition, if the service also requires a special app to be installed on the mobile device, then that app will also see any nonencrypted data before it is sent to the VPN service and potentially have access to other data on the mobile device. Thus, a free VPN service is much more likely to be tempted to exploit their access to non-encrypted data if that is their only way to profit from the free service.

One of the reasons for distrusting the security of a public Wi-Fi network is that you can never know whether or not it is supported by secure hardware

or whether that hardware is configured correctly to at least make it as secure as possible. Because of the limited number of users on one Wi-Fi network, the motivation to expend much effort to hack that one network is not high. But, if it shares an exposure common to many other Wi-Fi networks using similar hardware, it could be at risk. Furthermore, the users have no way of knowing the details of a particular public Wi-Fi node, so it is wise to err on the side of caution. A VPN service, on the other hand, may have hundreds of thousands of users.

The possibility that a free VPN service may be engaging in questionable behavior and be holding sensitive user data on its servers makes it an extremely attractive target for hackers and data thieves, who can justify spending much time and effort to break in. That makes any collection of sensitive information by a VPN service a more serious concern. One of the suggestions made is that you should look for reviews of a VPN service by known and trusted organizations before deciding on a VPN service. One of the interesting things that this data leak revealed was that there were several differently named free VPN services that all appear to be run by the same company. These were all supported by mobile apps that were gathering inappropriate data, combined with the attempt to disguise the company's true identity, suggest that this was a deliberate attempt to engage in unethical behavior. Caveat Utilitor

What Is a VPN, and Do I Need One?

By Joel Ewing, President, Bella Vista Computer Club

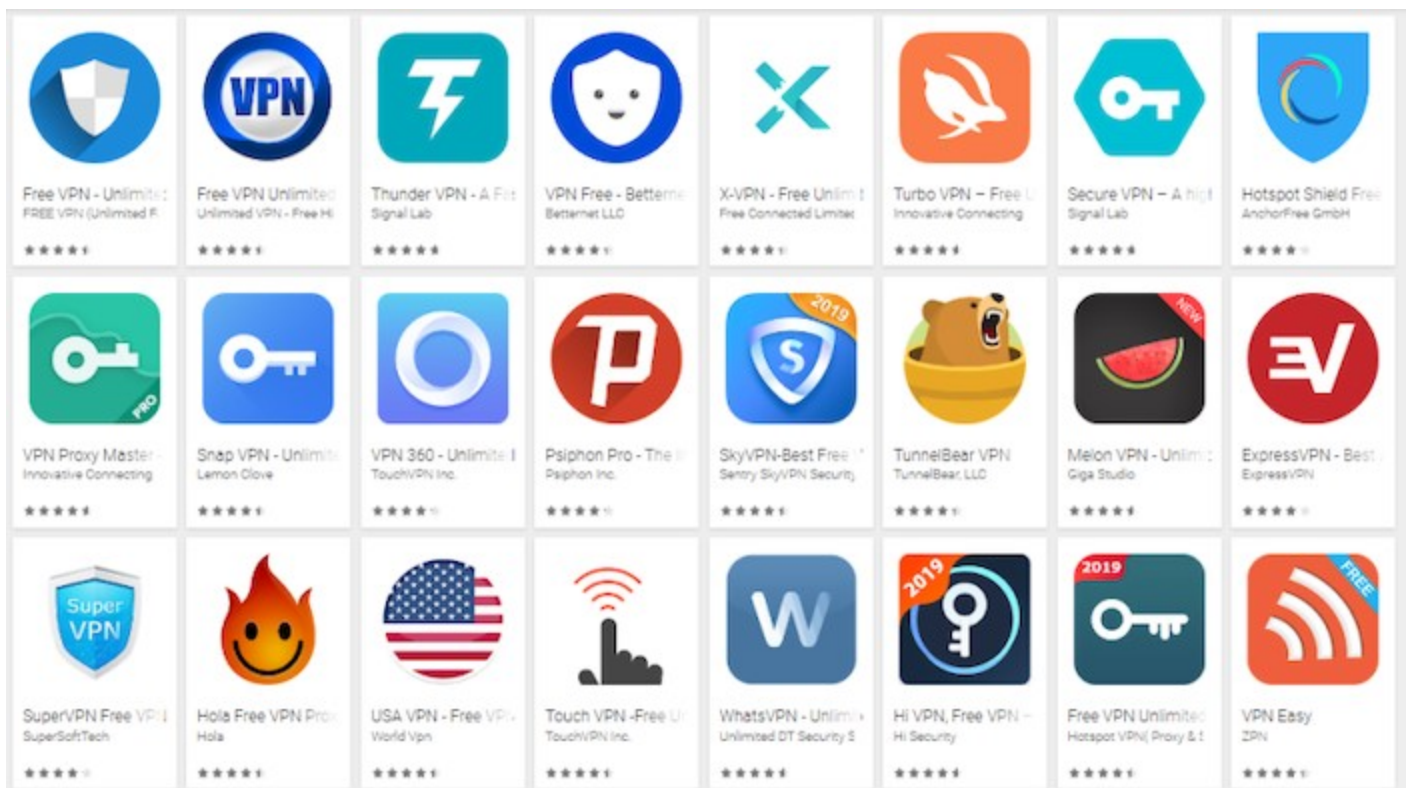
VPN stands for Virtual Private Network. When your computer or mobile device uses a connection to a VPN service, your device behaves as if it were connected to the Internet at the remote VPN service location, and all your traffic on the Internet appears to others as if it originates at that remote location.

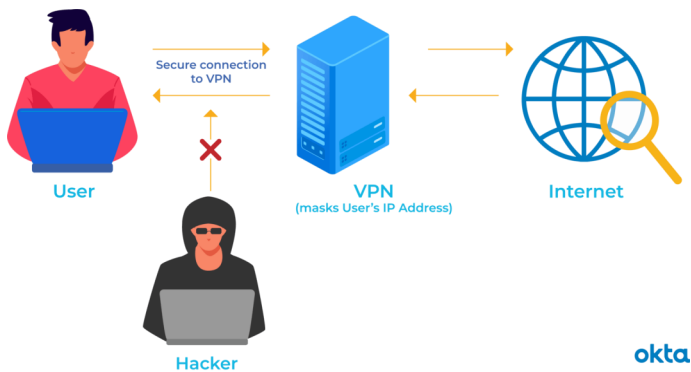
In actuality, the Internet service to which you are physically connected is used to establish a secure encrypted connection to your remote VPN service over the Internet. While the VPN service connection is active, your device is configured to reject any other direct network connections, so all inbound and outbound data flows through that encrypted VPN "tunnel" to the VPN server. The VPN server then establishes the final part of the path to the data's intended destination. Data that needs to be returned to your device flows over the Internet to the VPN server and then passes hidden over the VPN tunnel back to your device.

The logical behavior from the viewpoint of your device is as if your device were directly connected to the Internet through an Ethernet cable at the remote VPN server location. Your device is even assigned a LAN IP address on the remote site LAN. Others on the Local Area Network to which your device has physical attachment will be unable to establish connections in or out to your device while the VPN connection is active, and anyone seeing your data traffic either on your physical LAN or as it passes through any routers and the associated Internet Service Provider, will only see that you are communicating with your VPN service and be unable to read the encrypted data content. Note that if you are communicating insecurely with some website (like http vs. https), your communications will still be vulnerable on the Internet between the VPN Service and the destination website.

Reason for Using a VPN

(Continued on page 27)





(Continued from page 26)

Businesses that allow employees to work from remote locations may host their own VPN service to allow employees to access corporate network resources securely from a remote location. Suitable restrictions and conventions must be in place to ensure that devices that are not under direct corporate control that connects to the corporate network through VPN are suitably protected so they can't introduce malware into the corporate network.

People who do not use a corporate VPN service to work remotely use a VPN service, not to access resources in the remote network, but to use the remote network merely as a gateway to connect back to the Internet. If you choose to utilize insecure public Wi-Fi connections with your devices, then by default, anyone else connected to that same Wi-Fi LAN could potentially observe your data traffic, see what Internet sites you are contacting, and observe any un-encrypted data coming from or to your device. If the Wi-Fi network is compromised or misconfigured and there are any security flaws in your device vulnerable to network attacks, your device could also become compromised by malware. The use of a VPN greatly reduces the risks. If your device immediately enters VPN mode upon connecting to a public Wi-Fi, then attacks from other devices on the same local network are blocked, and the most someone else will be able to observe locally about your activity is that you are communicating with and sending unknown data to some specific VPN server.

If you are planning on traveling to a foreign country, you will probably discover that your email services block direct access from a foreign country to reduce spam abuse and that your favorite streaming services have region-specific content restrictions. If you have a VPN Service, you can circumvent those problems by using a VPN server in this country to make it ap-

pear you are still in-country, so normal email and streaming services still work. If you have a legitimate need to access foreign-only content, or perhaps a need to verify that some service is indeed blocked in a foreign county, then you can deliberately choose to connect to one of the servers your VPN service provides that is located in a foreign country. If you are accessing the Internet in a country under an authoritarian government that regards visiting some Internet sites as unacceptable, a VPN service could be part of a means to disguise unacceptable behavior; but under those circumstances, more than just a VPN may be required, as any obvious use of a VPN service could by itself be regarded as an intent to violate restrictions.

Available VPN Services

A search for "VPN services" will locate the most popular services. You may even locate some free services, but I would not be inclined to trust them. Remember that whoever is running the VPN service is the one who CAN observe all the Internet sites you are actually connecting to and any data you might send in un-encrypted form, and they have to fund their service somehow. That would have to be either by data mining for advertisers or restricting service in some way to encourage you to move to a paid plan.

Avast currently provides Avast SecureLine VPN service at an introductory rate of \$3.99 / month or \$47.88 for the first year (it looks like their regular price is \$89.99/year). Their service supports Windows, Mac, Android, and iOS devices on five devices concurrently.

NordVPN is a very popular service, currently available for a 2-year introductory offer of \$3.71/month, \$89.00 /2- years. Their regular price appears to be \$143.40 / year, making them much pricier down the road, but NordVPN also supports Linux operating systems and allows use on up to 6 devices concurrently.

Unlike an email service or an ISP service, which are a pain to change, changing a VPN service should be simple -- no identity change to communicate to others. Perhaps the best strategy is to use one VPN service provider until their introductory rate expires and then shop for the best offer available at that time.

Caveat Utilitor

Member's Area



BUSINESS CARDS



Pegasus
OPEN AIR PHOTOBOOTH

847.372.8186
pegasusphotos.smugmug.com

JIM JACOBS TRIO
Jazz Standards
THURSDAYS 6:00-9:00 PM

Deerfield
Italian Kitchen

CONTACT JIM AT 847.372.0656 OR JIM.JACOBS@MUSIC@GMAIL.COM

Hotline 

Phone: (847) 623-3815

Members 

Members Web Sites

e-mail me at editor@lcace.org

www.pegasusphotos.smugmug.com

 Take a good look, you just might see yourself.

LCACE Photo Albums





Liz Barnett
Chief Cookie Baker

Phone: 847-494-4222
E-mail: Liz@LoveMyCookies.com

www.LoveMyCookies.com
www.facebook.com/LoveMyCookiesLizB

Custom Cookie Treats for any Occasion!

Genealogy Your Way
Special Computer Services



Bobby Jacobs
847-372-0660

bobby@scs4now.com
scs4now.com

LAKE COUNTY HONOR FLIGHT

847.282.0374
info@lakecountyhonorflight.org



P.O. Box 1187, North Chicago, IL 60064
www.lakecountyhonorflight.org



Member of
The Association of
Personal Computer User Groups