Lake County Area Computer Enthusiasts
NEWS JOURNAL
VOLUME 34-07 January 2018 LCACE.ORG

Introduction to Personal Digital Security and Privacy

Presented by Robert Hurlbut
Meeting review by John Kinkopf, Member, Danbury Area Computer Society, CT
www.dacs.org
dacseditor (at) dacs.org

Our guest speaker at the August general meeting was Robert Hurlbut, an independent software security consultant and co-host of the Application Security Podcast. Robert delivered an excellent talk that covered many aspects of the wide field of software security. An expert in the field, he managed to provide lots of useful information without becoming too technical.

Asked from the audience which anti-virus software he uses, Robert answered rather provocatively: none! Most in the computer security field don't use an anti-virus software . . . . though he keeps Microsoft's Windows Defender on, included with Windows 10. Why? He explained that those in the security field live in a secure way, while anti-virus software usurps elevated privilege of one's system, more than any other application. We don't know if anti-viruses have faults in their code or security issues. And the majority of attacks these days are not the viruses of old, but things like ransomware that anti-viruses can't find, no way.

Updating Windows is essential to combat ransomware, and using Windows 10 over Windows 7 is his recommendation; definitely don't use Windows XP or earlier versions. Where a couple years ago there were 100,000 new virus patterns per year coming out; now it's 200,000 per DAY with which anti-viruses can't keep up. Thus, restrict your machine from executing things without your permission, meaning beware of clicking on things, and don't surf the internet as administrator, but rather in a user account. He also mentioned that there have been recent [but disputed] allegations against Russia-based anti-virus Kaspersky Labs.

Our connected world is a tracked world. Many TVs, home devices, and Echo or Home personal assistants listen to you. Many smart devices are security openings. Stores you enter may try to hook up with your phone's wi-fi to find out things about you. Credit card purchases leave footprints. [Yahoo scans my Trenton Computer Festival emails to pitch me "Meet Trenton Singles" ads. They guess and list my email recipient's phone number ("No, an out-of-state friend's church"), and "related contacts" as I compose.]

Private photos that iPhones backed up to the iCloud were obtained by fooling celebrity victims into divulging passwords with phishing emails. [Websites derive revenue from letting Facebook, Twitter, and marketing analysts observe which can be blocked by the NoScript extension for Firefox.]

(Continued on page 6)

LCACE January 13, 2018 demo presented by Chymna Rose Tececom Choices. Meeting at the Grayslake Public Library at 12:30PM. See you there.

"Members Helping Members"
(since 1983)

Board of Directors
2017-2018

Phil Bock . . . . . President
president@lcace.org

Linda Busch . . . . . .Vice President
vicepresident@lcace.org

Bobby Jacobs. . . . . .Secretary
secretary@lcace.org

Judy Dunham . . . . . Treasurer
treasurer@lcace.org

Linda Rohlfing . . . . . Programs
programs@lcace.org

J.J. Johnson. . . . . .Membership
membership@lcace.org

Linda Koudelka . . . . . Public Relations
pr@lcace.org

Volunteers

Webmaster . . . . . J. J. Johnson
webmaster@lcace.org

Newsletter Editor . . . . . Mike McEnery
editor@lcace.org

Historian . . . . Lester Larkin

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.

Lake County Area Computer Enthusiasts

LCACE
c/o Group Ambassador

"J.J." Johnson

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.

Phil's Ramblings

Happy New Year! I wish us all a peaceful, healthy 2018!

That said, 2018 is not starting out well for computer enthusiasts. The tech news as I write this column is all about a security flaw in Intel processors, which apparently affects most (if not all) of the processors they have sold in the last 10 years.

The technical details have not been fully explained, probably because remedial efforts have not been completed and those involved do not want to give any ammunition to bad guys who might want to exploit this flaw. However, for users like us the technical details of the problem are not all that important. What is important is that the flaw is in the chips themselves.

An obvious solution, common in auto industry recalls, would be to replace the defective part – in this case, the Intel processor(s) in your computer(s). However, at this point, no one seems to be talking about that as a solution. Instead, programmers have been busy working on operating system changes for Linux, Windows and Mac OS that will supposedly allow your computer to bypass the flaw embedded in your Intel processor. (Since we are now learning about this problem in the general press, we can probably assume that they are close to issuing their completed OS updates.)

While it is always important to keep your software updated, this takes on new urgency with this problem. Please be sure that your computer automatically downloads and installs system updates, watch for news about the release of an Intel-specific update for your OS and ensure that it installs properly on your computer!

Unfortunately, even with the eventual patch to our OS, we may not be out of the woods. This has to do with the relationship between hardware and software. From articles that I have read, hardware does things faster than software. Thus, there is speculation that once the software fix has been installed, it is very possible that your computer will run slower than it does now. It's early days, and much of that speculation has focused on large storage servers based on Intel chips. I'm sure that we will see more about this in the days to come, and thus be able to get a better picture of what we might expect once we install the eventual update(s) on our personal computers.

On a related note, there have also been recent articles in the tech media about security risks related to autofill functionality in our browsers and/or password managers. Most browsers offer to save logon information for you. If you agree, your browser will typically enter your user ID and password automatically the next time you visit that same website and are required to logon. Ditto for a dedicated password manager, such as LastPass.

The bad guys have figured out ways to exploit this autofill functionality. I will not try to explain the process in this newsletter; if you would like to learn more about the exploit, search online for "autofill security risks". The takeaway here is that we would be well advised to disable autofill in our browser(s) and password managers. The process will vary from browser to browser and password manager to password manager, so I encourage you to search on the web for instructions specific to your computer.

Moving merrily on to our next security risk, let's talk one more time about your router. Apparently, the bad guys have found a way to compromise router security through the Universal Plug and Play functionality built into many routers. Various tech experts have suggested that users disable this UPnP functionality in their routers.

Following this advice, I found a copy of the user manual for my TP-Link router and looked up UPnP information. Once I found the appropriate section, it was very simple to log on to my router and disable this functionality. I encourage you to do the same.

(if you would like more information about this new risk, please search the web for "router UPnP vulnerability".)

Sorry for all the bad news! Sadly, it appears that 2018 is likely to see the same stream of security issues that we saw last year. The bad guys are still out there, they are getting smarter and they're probably becoming more numerous (as they entice "newbies" by offering scam training and "rental"). We too must become smarter, and remain vigilant!

All the best!

LAKE COUNTY AREA COMPUTER ENTHUSIASTS

Annual Prize Winners

First Prize—Harriet Rudnit

Harriet won an Ausus Notebook Computer with 15.6 in LED Display

2nd & 3rd Prize—Todd Porthouse

Todd won $50.00 and $150.00 gift certificates

Winnie Frost won the 50/50 Raffle

Sweater contest Judges

Ugly Sweater Winner Diane Carlson Most Creative Sweater DeBorah Sirilla.

(Continued from page 1)

Showing an RFID shield, Robert told how his Fitbit activity tracker began flashing numbers and making strange noises at the DEF CON hacker convention. Though visitors are warned to turn off any Bluetooth device at hacker conventions, a Fitbit's listen remains on. He's refraining from connecting it to anything until he can test it for tampering on a laptop he can wipe.

Get rid of many routers known to have vulnerabilities. Buy your own wi-fi equipment, using your own router over those an ISP provides, so you're managing your wi-fi instead of them. Use WPA 2 for your home wi-fi encryption; DON'T use WEP.

Virtual Private Networks (VPN)
To provide a secure channel to network servers over the internet, companies commonly use Virtual Private Networks for off-site workers. Phones can also be connected by VPN. Free personal VPNs offer privacy, not anonymity — you pay by providing info of your use that may be sold. Robert advises, nothing is free; don't use a free VPN. Use VPNs when you can, and only reputable pay VPNs [$60-$120/yr]. [Websites rate VPNs.] Robert subscribes to F-secure Freedome; it logs attempts stopped to track you and how much transmitted data was protected; they've been a reputable provider for 25 years. PIA is a VPN recommended by publications as doing minimal logging of the user's IP address and usage. For banking Robert answered that he would use a VPN, but they raise banks' suspicions of your authenticity. Asked about using a VPN to bypass media play geo-restrictions, Robert followed up by email that he once used ExpressVPN, and gave these references:

https://thevpn.guru/how-bypass-geo-restrictions-location-errors/

https://www.bestvpn.com/best-bbc-iplayer-vpn/

Audience members pointed out that governments may require VPNs to provide their logfiles of users. A VPN user in the audience shared that PIA's encryption processing made his battery life prohibitively short, in his experience. OpenVPN is open source; keep its patches up-to-date. OpenVPN how to: https://openvpn.net/index.php/opensource/documentation/howto.html

Browsers > Tor > Tails
Unfortunately, browsers track you. While Apple is good at security, their Safari browser lags; but, at least it excludes Flash, notorious for having security and reliability issues. [July News Flash: Adobe will pull the Flash plug-in in 2020.] Search engine DuckDuckGo.com claims not to track you . . . they say. URLs beginning with https provide improved communication security over http sites.

By relaying online communication through multiple nodes on its volunteer network around the world, free download Tor (The Onion Router) anonymizes a web surfer's identity and point of origin. Once the route for each use is established, one surfs the internet via Tor's modified Firefox browser – during which all other browsers must be closed for Tor's anonymity to be effective. Downsides are that while preserving your web anonymity on your end, many websites recognize Tor exit nodes, and place restrictions. For example, Wikipedia restricts edits made through Tor; BBC blocks its use to access iPlayer. And Tor's practicality is limited by slowed browsing from bouncing communications around multiple anonymizing nodes in world locations of varying internet speeds. Only download Tor from the Tor Project website: https://www.torproject.org

Tor is used to access Tor sites on the dark web which Edge, Google, and Chrome won't. Because it's possible that data may still unmask you, the next step is to use Tor in Tails.

Tails (The Amnesic Incognito Live System) is a live operating system the user boots from a USB drive or DVD for the purpose of having no connection to anything on the PC, say a library PC, just the network. When your session is finished no data is saved, everything is anonymous, and traces are not left when you disconnect. But associating with, for example, your email or Facebook would give you away, of course. As using your home computer would identify you to your ISP. It's better to get a dedicated laptop with completely separate email and other accounts that you never use in ways to identify you. The Tails website: https://tails.boum.org

(Continued on page 7)

(Continued from page 6)

Passwords

Early August News Flash: Robert Burr, responsible for the 2003 recommendation that secure passwords include upper and lowercase letters, and symbols that render remembering passwords difficult, made the media rounds rescinding the suggestion, or "|\|3\/ €R /\/\1|\|D." His, and Robert's current thinking is to use long passphrases – passwords composed of words strung together into a nonsense phrase you can remember. [For example, "A wet duck only flies at midnight," "The blue sun melts the wet snow" – from TV's "Get Smart"]

The "Have I Been Pwned?" website is a free service to which one submits their email address. The site, maintained by Australian Troy Hunt, will reply if the account is found among the millions breached, along with when, what, and where it was found, say perhaps in Pastebin, where a lot of stuff happens. You may also sign up for its Notify Me service, to be notified in the event future account compromises are found, for which Pwned needs to save your email. Robert has met Troy; the site gets some financial support but he does this mainly as a labor of love. Website: https://haveibeenpwned.com

A Password Manager (software) helps you manage your passwords with one master password that should be chosen to be especially difficult to crack. Password Managers can also manage security questions. Security question answers you choose need not be truthful, and should not be obvious. The password manager Robert uses is Blur, often recommended in books, which also can create virtual credit cards for you. Blur hasn't shown up in any breaches or other problems, while 1Password and LastPass have had reported security fallibility.

Two-factor authentication (2FA)

An example: Upon entering my account password, YouTube requires that I submit a code sent to my email (or phone). Robert likes it; I feel my YouTube account is more secure. But he thinks that it's crazy to give oft-hacked Yahoo his phone number. The website TwoFactorAuth.org lists whether or not websites support the additional security of 2FA.

Email

All emails are wide open. [Like my ballot at the Putnam County polling place!] They are transmitted from server to server, where hackers can view them along the hops. Even if you delete an email, the email services have made copies for sending redundancy. Be wary of clicking on email links and attachments. For privacy consider premium email services based outside the U.S. that encrypt. OpenPGP.org can be tried for encryption. A member of the audience reported using it in Gmail. The cable email accounts are worse regarding sharing your email information. Don't ever send forms with your social security number via email. [Send word documents only as PDF files, for with Word file hidden histories a recipient could work back all your revisions, back to the resume I started writing this review over!]

Credit Cards

Robert said your health care records are worth even more to criminals. Check your credit report annually, at the beginning of the year. A few months later check Experian and Transunion for whether anyone is opening an account in your name. Robert found someone had opened an account under a previous address. One can download them or receive them by regular mail, but don't have the reports sent by email. Consider putting fraud alert and credit freezes on your credit card.

Beware of credit card skimming. July News Flash: wafer-thin "insert skimmers" stealing bank card information at ATMs are proliferating. August News Flash: tiny gas pump skimmers transmitting credit card information, as Robert mentioned, are featured on TV news. Robert mentioned that credit cards with chips are partially better, but not as good as in Europe, where a PIN is required, too. At locations credit card skimmers target, it's better to use a prepaid card or Apple Pay. But Apple Pay's one-time token uses near field communication (one needn't contact, but be in proximity) and there are devices the hacker can use to connect and obtain information.

Iconic hacker Kevin Mitnick advises having someone else buy your debit cards so video cameras don't record that it's your purchase. NSA whistleblower Edward Snowden did this, along with using Tails.

Mobile Security

Update to the latest operating system version and patches. [Ha! Google no longer supports Android versions predating 4.4.] For iOS definitely get the latest version, 10.3.3, which

(Continued on page 8)

(Continued from page 7)
patches a chip vulnerability that was exploited at the Black Hat hacker conference. Passwords or passcodes protect your device. Adjust your permissions per app to, "No, no, no, no." Robert keeps his Uber car service location permission set to Never, except for the few minutes he needs to switch the permission to Always to use the app. Robert answered how to, for an Android phone, go to Application Manager, click on the app, and it should show you the permissions, at least since the 6.0.0 Marshmallow release. Anything version 5 or below, you couldn't do this. For Android, you definitely want an anti-virus. Sync, back-up your data, and install a phone finder app. It is very important to turn off wi-fi and Bluetooth when you're not home or not around trusted endpoints, which is nearly everywhere. Turn them off when they are not needed.

Pineapple is a popular device at the hacker conferences. If your phone has ever been connected by wi-fi it retains that information, and connects when in range to any of them when its wi-fi is on. The Pineapple connects to your phone, without your knowing, by pretending to be one of its former wi-fi connections.

The most secure mobile phones are the basic flip phones, turned off [in an RFID shield]. Tether your mobile phone to a hotspot in lieu of wi-fi or Bluetooth. Law enforcement uses fake cellular towers to spy. [August News Flash: Android messaging apps were found carrying SonicSpy trojanware to spy on audio, take control of phone cameras, and nearly all of a phone's functions.]

Security News Sources
Robert said that he keeps current by following several security news sites on Twitter. KrebsOnSecurity.com is an oft-referenced website, widely sourced when it detailed how customer accounts were hacked though Target's air-conditioner computers. [One can subscribe to his email newsletter.] Robert has Google searches set up to feed emails when certain terms come up such as router or VPN. One audience member subscribes to Wire's news feed, another visits https://www.social-engineer.org .

Books Robert Recommends
The Complete Privacy and Security Desk Reference: Volume 1: Digital – Michael Bazzell and Justin Carroll

Hiding from the Internet: Eliminating Personal Online Information – Michael Bazzell

Personal Digital Security: Protecting Yourself from Online Crime – Michael Bazzell

The Art of Invisibility – Kevin Mitnick

How to Be Safe in the Age of Big Brother and Big Data – Kevin Mitnick

iPad and Smartphone Together at Last

iPad and Smartphone – Together at Last
Presentation by Gabe Goldberg, APCUG Advisor, Region 2
Meeting Review by George Cadmus, Treasurer, Northern Neck Computer Users Group (Virginia)
September 2017 issue, The Computer Link
http://www.nncug.net/
Geocadjr (at) verizon.net

Gabe started the presentation by giving his experiences with a tablet and smartphone. It was about six years ago that he decided to purchase an iPad just for the experience of having one and to see what they were all about. He wasn't quite sure which iPad to purchase and decided on the middle of the road and purchased the 32 GB model.

Gabe advised over the course of his computing life he has obtained a bookcase full of manuals from purchasing other computer equipment. He was very surprised when he opened his new iPad box and found that it did not contain any documentation or instruc-

(Continued on page 9)

(Continued from page 8)
tions on how to operate it. Gabe advises if you are looking for help with your iPad, there are many sources you check printed help books that are available at book stores and Amazon; you may even find some manuals at your local library. You can also obtain help by visiting online help sites. If you have a local Apple group in your area, you may also seek help from them.

About Apple Care, Gabe decided not to get a policy, as in his opinion it was not worthwhile. He opted to purchase the Wi-Fi only iPad instead of one with cellular connectivity. Setting up the Wi-Fi connection was simple. Once you set up your Wi-Fi connection, it will remember your network location. Gabe advised it was a good idea to check your privacy settings to stay safe. He also suggested you keep your apps updated.

After using his iPad for some time, it was now time to get a new upgraded iPad. To get the new iPad, he convinced his wife that it was time for her to get an iPad and he started showing her what she could do with the device. Gabe's wife agreed that she would like to have an iPad as it seemed very interesting. So, Gabe gave his wife his old iPad and he was now able to purchase a new one for himself.

Gabe told he used a flip phone for a long time before purchasing an iPhone. The flip phone did everything he wanted it to – it made and received telephone calls! Verizon even sent free digital phones to both him and his wife.

In 2016, he decided it was time to update his phone and purchased his first iPhone. He purchased an unlocked iPhone at an Apple store. The sales person was pleasant but the telephone was expensive.

The sales associate started out the conversation by asking Gabe what his needs for the phone were going to be. Once finding out what Gabe needed for his phone, the sales associate suggested several models. Gabe opted for the larger 6S Plus. An advantage of purchasing a phone at an Apple store is that they provide basic free classes on how to use the phone and provide some tips and techniques.

To register for an Apple account was quick and easy. Gabe opted to use Consumer Cellular as his carrier. He gets 250 minutes and 1.5 GB of data to share with his wife each month. The cost for this plan is only $47 a month. Also with a Consumer Cellular account, if you go over your allotted 1.5 GB of data, Consumer Cellular ups your data plan to the next tier for only one month. After that, it goes back to the original data plan. Gabe exceeded his plan one time and was moved to the next tier which only cost him an additional $9. Prior to signing with Consumer Cellular, he was a long time Verizon wireless user. Consumer Cellular was easy to set up.

They have great customer service with flexible and economical call/data plans. They also have a great referral bonus plan that rewards you $10 for every person you recommend to Consumer Cellular. Before you can use Consumer Cellular, they will send you a small circuit card that you must insert into your phone.

Gabe reported that there are many apps for your phone. There are way too many apps to just browse, and you should seek suggestions and recommendations of which apps you would like. Before downloading apps, you should check the ratings and reviews. If you see a lot of bad reviews, you probably shouldn't download that app. You should take note when the app was last updated. Also, be careful and make educated choices when choosing an app.

There are many free apps to download. There are also many you must pay for. Sometimes it is important to remember, "You get what you pay for." It is also important to support the app developers. They are providing you a service and for them to continue their work, a contribution to them should be considered.

With your iPhone, and if you are a customer of a cable company, you can watch their TV channels on your iPad and iPhone. You can also watch movies on your devices.
Some of Gabe's favorite apps include a navigation app called Waze. Waze will give you directions to a location and will also track traffic in real time. This can help you if you become bogged down in traffic. It will offer you an alternate route. This information is ob-

(Continued on page 10)

Membership

Report will be back Next Month

Donna Kalinoski

&

Roger Busch

(Continued from page 9)

tained by other drivers on the system. He also uses Keynote, Safari-Firefox-Chrome, Life 360 and has also tried virtual reality. To help other users who may be contemplating downloading an app, you should consider rating the app that you are using and share your experiences both good and bad.

Gabe gave some usage tips for the phone which include closing all apps that you are not using. Also delete any apps you no longer use. You should use an ISP Wi-Fi hotspot to save some of your bandwidth. With newer vehicles, you can connect your phone to the vehicles with the built-in technology.

You can connect via Bluetooth and also by using Apple Play. Other tips included using your charger when using a navigation app with your iPhone as your phone battery may die before reaching your destination. You should also consider a speaker and earbuds for your phone. You may also want to consider getting a hip case for your phone for comfort and accessibility. You should also add your contacts to your phone so you will always have the numbers handy. You may also want to explore the world of texting. One other tip to consider is setting up “find my phone” in case your phone is lost or
stolen. Voice recognition is another thing to consider.

On the subject of purchasing an Apple watch, Gabe reported that he has no interest of ever purchasing an Apple watch as the screen is much too small for him. The iPhone is about the smallest screen he would ever consider.

Gabe ended his presentation by telling the group if they ever have any problems with their equipment or programs, they should consider using Twitter to complain. He advised he was having problems with is Verizon service and used his Twitter account to contact the CEO of the company. Gabe reported that he did receive a reply from Verizon and the problem he was having was solved. He said that companies have personnel that monitor social media and can help if you have any problems.

We thank Gabe for the wonderful and informative presentation.

Lake County Area Computer Enthusiasts

Do you have computer questions
or need help with your computer?

Visit Lake County Area Computer Enthusiasts'
help desk for one on one help

Open to all

11:15 a.m.-12:15 p.m.
Grayslake Area Public Library
Rooms A-C

Hotline **L.C.A.C.E.**

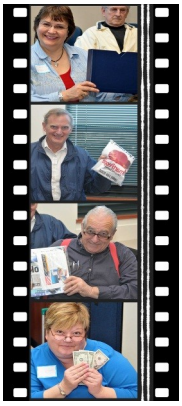
Phone: 847.623.3815
Web Site: http://www.lcace.org

Members

Have your Web Site Advertised here,
e-mail me at editor@lcace.org

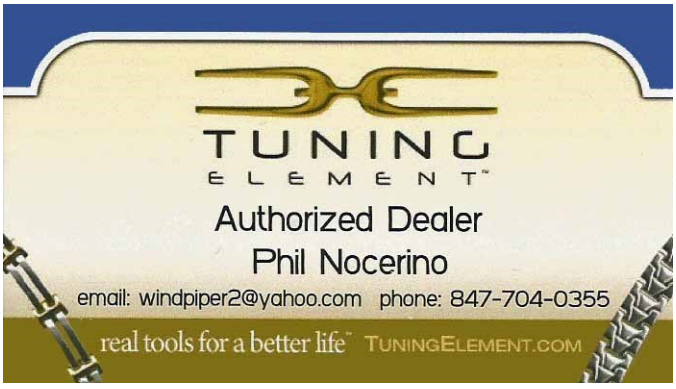
www.pegasusphotos.smugmug.com

www.RobinSeidenberg.com



Take a good look, you just might see yourself.

LCACE Photo Albums

apcug
Member of The Association of Personal Computer User Groups

Pegasus
Event Photography
5 Minute PHOTOS
Dwight "J.J." Johnson
Photographer
847.623.3815
info@pegasusphotos.net
View & Order: pegasusphotos.zenfolio.com