

Reaching Out From a
Common Experience

"Reaching Out From a Common Experience"

Greetings from a unique group of people - the retirees of the Los Alamos National Laboratory (LANL). The Laboratory Retiree Group (LRG) is a non-profit corporation which seeks to maintain communications with and to serve the needs and interests of retirees from LANL. If you wish to join our organization, an application is available in this newsletter. For more information, please contact our President Charles R. Mansfield at coyote2@swcp.com or by mail at P. O. Box 546, Los Alamos, NM 87544.

LRG Officers and Board Members

President: Charles R. Mansfield coyote2@swcp.com

Vice President: Dale Thompson dalethompson@losalamos.com

Secretary: Mary Menzel jlmenzel@netzero.com

Treasurer: John Stewart jns@rt66.com

Board Member: George Best georgehbest@cs.com

Board Member: Norman Delamater ynormdel@earthlink.net

Board Member: Sheila Girard sgirard@losalamos.com

Board Member: Lester R. Hoak mhoak@q.com

Board Member: Mary L. Mariner

Board Member: Bob Meier bobmeier@mac.com

Board Member: David Schiferl dsconsult@centurylink.net

Board Member: Cecil Stark cecilstark@gmail.com

Board Member: Alan Wadlinger awadlinger@vla.com

Committee Chairs

Health Issues: Glenn Lockhart, (505) 672-3784, and Ken Wilson, Co-Chairs

Health Care Premium Working Committee: Glenn Lockhart

Computer Literacy: Mary L. Mariner, (505) 672-1950

Membership: Sheila Girard, (505) 672-3497

Main Gate: John Stewart, (505) 662-7158

Web Contact: LRG Web Master: Don Reid lrg271a@gmail.com

The **Laboratory Retiree Group** web site is www.losalamoslrg.org.

Don't be the easy hack

By: Chris McGee, VP of Information Technology at Del Norte Credit Union

I'm sure you have antivirus software on your home computer, right? So you are protected, right? I wish it were that easy. This past year, an executive at Symantec, a leading antivirus developer, announced that antivirus solutions are only about 45% effective. Zero-day exploits or viruses that are not known to software manufacturers or malware that can be easily modified to "look" different to antivirus applications are sold on black markets on the internet and make it easy for hackers to get a hold of malicious applications to use. Add to that that it takes an average of 4 days for an antivirus developer to patch their software and you need more than an antivirus application to protect you. Patch, patch, patch. Unless you are an internationally known multi-millionaire, chances are you are not going to be the first to be hit with a new exploit. Software manufacturers constantly are responding to holes that have been identified within their software and they release updates to combat these identified security issues. Set your software to auto-update or stay vigilant in updating software. Microsoft or Apple security updates are a must, but also look at other software you have installed on your computer such as Java and Adobe. Many of these products are used in the background when you are surfing the web and webpages can have exploits that use this software to gain access to your system.

The best defense on your home computer is to assume someone will get on your computer. To combat this, the use of a backup disk and encryption applications can protect you. Most people don't use confidential documents on their home computer every day so backing up important documents to an external disk is not that cumbersome. A cursory look on some on-line computer hardware sales sites shows that you can get a very large external hard drive for about \$65. If the disk isn't connected, a malicious attacker can't get to it. So only connect the external disk with critical information when you need it.

A great resource for data encryption can be found here (<http://www.gfi.com/blog/the-top-24-free-tools-for-data-encryption>). Encrypt tax returns and other sensitive information or better yet use full disk encryption. Tired of remembering passwords (more on that in a minute), use an encryption tool to store passwords and then have one master password to get to that list. There are web versions such as LastPass or desktop versions such as KeePass. If you need to transport data on USB drives or other removable media such as an external hard drive, Rohos Mini Drive encryption can protect that data. There are many tools out there for many different uses, just find the right one for you.

Now that we know of a way to store all these passwords securely we can stop using the same password for everything. Having the same password for your Twitter account that you have for your home banking is a big red flag. Twitter doesn't safeguard your password to the extent your financial institutions do. Hackers have been known to hack social media accounts, grab the usernames and passwords and then try many different banking websites to see if they are the same. You would be surprised how often they are. As most of you know your financial institution passwords should be very complex. Uppercase, lowercase, numbers, and symbols should all be used.

Social media is a hacker's playground. The amount of information people freely give out to others is scary. Think of common security questions that you see on websites; What is your favorite pet's name?, Where did you grow up?, What was your first car?. People on social media share this information all the time with people they hardly know on the internet. Hackers know this and target people's personal information from people in order to social engineer information from them. The best solution is of course don't share this info on-line, but another option is that when you sign up for a website that requires security questions come up with a list of answers that have nothing to do with the answer. What is your favorite pet's name? Chair. What is your favorite color? Window. In other words it doesn't matter what someone knows about you they will never guess your answer and

(continued on page 3)

(continued from page 2)

now that you have that encryption software installed you can store those answers in there as well. The majority of hackers are not going to seek you out and attack you. Hacking is a numbers game which is why most people are attacked through email and the web. The first step for protection is to know what you are clicking on. In email, only open an attachment only if it is from a known person and you are expecting the document. Check to make sure the email address is really the sender that it is supposed to be. It is easy to create fake emails such as joesmith@w.gmail.com. A quick glance and you might say that is my friend Joe Smith from his Gmail account but that "w" in front of "gmail" means that it is coming from a completely different location. The same can happen with links in email and webpages. If you hover over links you can tell where they really take you. It might look like the link is taking you to www.supersafesite.com but when you hover over the link it is really taking you to www.iwillhackyou.com. The smart play is if you know the person sending the email such as from your financial institution with a link to view your statement, simply go to your financial institution's website log-in and look up the statements without clicking on the email link.

Also be vigilant in what you say over the phone. Don't give out personal information to people that call you. If someone calls and asks for information ask them if you can call them back. Take down their number and search on-line to make sure it actually came from the person or company that they say they were. The credit union will not call you and ask for you to verify your account information or your online banking user name and password so don't give it out. If you have concern it doesn't hurt to be cautious.

The Bureau of Justice states that there were 16.6 million people that experienced identity theft in 2012 and this number continues to grow. There are two websites, www.us-cert.gov/ncas/tips and www.balancetrack.org/identitytheft/index.html that have a plethora of information on identity theft. If you suspect you are a victim of identity theft call your financial institutions and the major credit bureaus immediately as they can put an alert on your account to where more in-depth attention is paid to attempted new lines of credit or purchases.

The bottom line is most hackers want the easy hack. They don't want the hassle of going around security measures; they want to find the victim that hasn't paid any attention to their security and are easy targets. Just like the burglar who won't go to the house with a barking dog and an alarm system when they can go down the street to an easier target. If you are vigilant with your security and cautious with your information you become the hard targets that hackers don't want to spend their time on.

11,600 Blue Cross Members Affected

(from the Albuquerque Journal, February 25, 2015)

Blue Cross Blue Shield of New Mexico announced Tuesday that 11,600 of its current or former members were affected by the data breach at health insurer Anthem Inc. on Feb. 4. It said some of those affected had their Social Security numbers exposed.

"Some members may have been traveling and may have accessed an Anthem network or may actually reside in an Anthem state and have Blue Cross Blue Shield of New Mexico coverage due to an employer or living situation," said Blue Cross spokeswoman Becky Kenny.

The company will send notices within the next few weeks to those affected.

Blue Cross is a separate company from Anthem, but the two collaborate through various agreements.

A blind man walks into a bar, taps the man next him and says, "Hey, wanna hear a blond joke?" The man said to the blind man, "Look buddy, I'm blond. The man behind me is a 400-pound professional wrestler, and he's blond. The bouncer is blond. The man sitting over to your left is also blond. Still wanna tell that blond joke?" The blind man was silent for a moment and then said, "Nah, I wouldn't want to have to explain it five times."

Christmas 2014 (Photos from Los Alamos Daily Post)

Christmas Parade (l to r) - 1st row=1st & 2nd (tie) place; 2nd row=2nd (tie) & 3rd place

The next two are the same house with a different light schemes. The bottom is a house on Barranca Mesa.



Same
↔
House



WINTER 2015

(Photos from Los Alamos Daily Post)

Rock Balancing At Ashley Pond



Snow fall - January 14



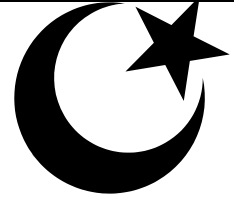
Snow fall - February 11





LANL In Memoriam

10-29-14– 02-22-15
By Jack Clifford



David M. Smith	Keith E. Dowler	Shirley A. Vandergust
Paul R. Farrell	Pharis Williams	Pauline Stone
Orlando (Butch) M. Smith III	Howard C. Volkin	William C. Robbins
Paul Weiss	James S. Hena	Samuel J. Bame, Jr.
Barbara G. Troupe	Carolyn A. Edwards	Alphonse Popolato
Henry Horak	Henry Montoya	Marvin M. Mueller
Annabelle Honnell	Donald J. Liska	Edward G. Arntzen
Teresa B. Smith	Ben Cody Benjamin	Jesse V. Cordova
Jeff H. Torrez	Earl A. Meyer	Jeannie A. Stein
Joseph Bubernak	James D. Moss	Thomas J. Humphrey
William M. McCall	Lorenzo "Lenny" Barrone	

Health Issues by Glenn Lockhart

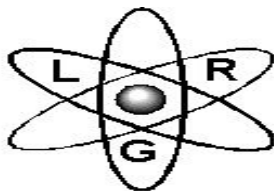
I have received a suggestion to discuss the change from AON Hewitt to Empyrean Benefits Solutions on April 1, and the Anthem Blue Cross Blue Shield security breach.

Change to Empyrean: This is NOT a change of health insurance plans. Empyrean will be acting for LANS in determining eligibility for health insurance benefits (health care, dental, eye care) and legal insurance; will act for LANS in enrolling retirees in appropriate plans upon retirement, enrollment in Medicare, and during Annual Open Enrollment; disenrollment of retirees upon death or other events; and administer retirement benefits for LANS (NOT UC) retirees. Both LANL Benefits and AON Hewitt assured me that a mailing would occur sometime before April 1 which explains what retirees are expected to do for the transition. One possibility is to require retirees to re-register on Empyrean's website.

Anthem security breach: This should have minimal exposure from an identity theft standpoint. The only exposure that I can identify is if you were enrolled in the UC Core plan prior to 2010 (administered by Anthem); or were not covered by Medicare, enrolled in a Blue Cross and Blue Shield of New Mexico Plan (late 1990's, 2010 to present), and received services from a California provider during that period. Normal precautions against phishing and scamming should guard against identity theft.

Retiree contacts since the last *Main Gate* reminded me that I have not discussed spousal Medicare eligibility for some years. Many retirees do not realize that they can be eligible for Medicare Part A (without a premium) based on their spouse's (or ex-spouse's) work history. If the retiree is not eligible for Medicare Part A on their work history but is eligible on their spouse's (or ex-spouse's) ac-

(continued on Page 8)



Reaching Out From a
Common Experience

LABORATORY RETIREE GROUP (LRG) MEMBERSHIP APPLICATION

LRG has two classes of membership. Participation in all LRG social or educational events is open to **all members regardless of membership classification.**

ACTIVE Member: A Los Alamos National Laboratory employee who has retired from a prime contractor of LANL (UCRS, PERS, LANS or OTHER). Active members pay dues of \$12.00 per calendar year, have voting privileges at Annual Meetings, and are eligible to serve as LRG Officers and/or Directors. Active Members receive copies of the LRG DIRECTORY and LRG's publication, *The Main Gate*. A spouse (or ex-spouse) may become an Active Member upon death (or divorce) of the Active Member with payment of \$12.00 yearly dues.

FRIEND: A person who is not a LANL retiree but supports LRG. Friends pay dues of \$15.00 per year to cover the cost of printing and postage for the DIRECTORY and issues of *The Main Gate*. Friends cannot vote or hold office.

THE LABORATORY RETIREE GROUP, INC. (LRG)

- ☐ New Membership ☐ Renewal ☐ Friend ☐ Change of Address
☐ Check here if requested information remains unchanged (including phone no. and e-mail)
☐ Check here if you DO NOT want to be listed in the DIRECTORY

Lab Retiree: _____, _____, _____ Year Retired _____
(Last Name) (First Name) (MI)
System: UCRS PERS LANS OTHER (circle one)

Spouse: _____, _____, _____ Retiree? Year _____
(Last Name) (First Name) (MI)
System: UCRS PERS LANS OTHER (circle one)

Friend: _____, _____, _____
(Last Name) (First Name) (MI)

Address: _____ **City:** _____ **State:** _____ **Zip:** _____

Telephone: () _____ **E-mail?** No Yes: _____

Payment: Please send dues payment by check to the following address:

LRG, PO Box 546, Los Alamos, NM 87544

Check#: _____ Date: _____ Dues _____ Los Alamos Employees' _____
Amount:\$ _____ Scholarship Fund Donation:\$ _____ Total:\$ _____

Laboratory Retiree Group
LRG, Inc.
PO Box 546
Los Alamos, NM 87544

PRESORTED
STANDARD
U.S. POSTAGE PAID
LOS ALAMOS, NM
PERMIT NO. 152

Address Service Requested

(continued from Page 6)

count, LANS requires the retiree to sign up for Medicare Part B. Every LANL retiree is eligible for Part B on their sixty-fifth (65th) birthday and must enroll in Part B during the seven month period around their 65th birthday (or retirement date, whichever is later) to avoid the Medicare late enrollment penalty. Medicare charges a late enrollment penalty of 10% of the Part B premium for each twelve (12) month period after the required enrollment date based on the 65th birthday or date of retirement). The problem that is created comes from not signing up for Part B on your required enrollment date; having a much younger wife (who must be at least 62 for spousal eligibility to apply); and having to pay the late enrollment penalty to keep LANL insurance.

Example: Man retired at age 60. Man has 20 quarters under Social Security, his spouse has 40 quarters. The spouse is a dependent on the man's LANL plan (she may be eligible independently if she is a LANL retiree). Man is 84, spouse is 62 when he realizes that he has to sign up for Part B and pay a monthly premium of \$104.90 plus 190% of \$104.90 (\$199.31) to keep LANL insurance. The Part B premium and resulting penalty can be higher, depending on income.

Keeping LANL insurance is STILL A BARGAIN, even with the late enrollment penalty.

If you have a question about health care or other benefits, call me at (505) 672-3784, e-mail at mandmlockhart@cs.com, or snail mail at 91 Mimbres Drive, Los Alamos, NM 87544.

Coffee and Conversation (and Breakfast)

1st Tuesday of the month, 8:30-10:30 a.m.

Viola's on Trinity.

Coffee is free.

Annual Meeting and Meal
Saturday, May 16, 4:00-7:00 p.m.
Location unknown presently
Postcard will be sent