

BREA NEWS

<https://bera.bnl.gov/brea/>

Volume 26, Issue 3

May/June 2026

BREA Meetings

BREA meetings are held on the second Tuesday of every month (except for August), at 1 p.m. All BREA members are invited to attend and participate.

Zoom meetings via video link have become the norm. Contact any officer for help to join a meeting.

Meeting Schedule

May 12, 2026

June 9, 2026

July 14, 2026

BREA Officers

President

Arnold Moodenbaugh
moodenba@optonline.net

Vice President

open position

Secretary

Laura Miller
lj96miller@outlook.com

Treasurer

Louise Hanson
hanson.louise@gmail.com

* * *

Newsletter Editor

Mona S. Rowe
msrowe.hi@gmail.com

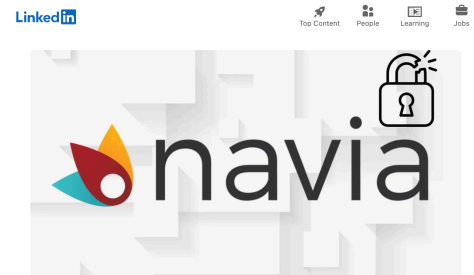
From the President

by Arnie Moodenbaugh, moodenba@optonline.net

To BREA members,

We are sad to announce the recent passing of our BREA Vice President Andrew Feldman after an illness. We were informed via a short note from his son. Mona Rowe has written a sympathy card to the family on behalf of BREA. Andy joined BREA ten years ago and was an active member, serving as Vice President since 2024. At a Zoom meeting that same year, he gave a memorable report on his flight to conduct a photo reconnaissance the day after the 9/11 attack on the World Trade Center.

This issue features a discussion of on-line fraud and some strategies to avoid getting entangled with the criminals perpetrating it. You will find advice from authoritative sources, as well as anecdotes from BREA members. Recently, Navia, the company that manages retiree health benefits for BNL, had a data breach involving personal information, including name, date of birth, Social Security number, phone number, email address, and health plan information for impacted individuals. If you have a health reimbursement account (HRA) with BSA, you should have received a letter in the mail from Navia describing the extent of the breach. You can also review the information at <https://www.naviabenefits.com/notice-of-data-event/>. Navia does indicate that banking information was not divulged (whew!). We can have additional discussion at our May 12 meeting. We intend to schedule a presentation by an expert on cybersecurity issues for a future meeting.



Navia Confirms Data Breach Exposing Sensitive Information of 2.7 Million Users

(continued on p. 4)

Elder Fraud, Phishing, Deepfakes . . . Oh, Oh!

Can you spot scams? See an impersonator scam that came to Betty Elder.

Hi Betty,

I'd like to know if you're available. Louise needs to pay a vendor today, but doesn't have Zelle, Venmo, CashApp, Chime or PayPal. Please let me know if you can help me pay with any of these platforms. It's an association expense program and it's urgent. Louise will send a reimbursement check if you can help. Please get back to me as soon as you receive this message.

Best Regards

Arnold Moodenbaugh



Betty Elder is BREA's membership chair and Louise Hanson is BREA's treasurer. Elder replied with a simple query to the sender, Arnie Moodenbaugh, BREA's president.

Then she got this:

Thanks, Betty. The amount is \$1,062. Please let me know if you can cover that.... Louise will ensure to send you a refund check as soon as the payment is processed, if that is preferable.

Now Elder was getting suspicious. She checked the email address of the sender. It did not match the address she had on file for Moodenbaugh. Ah hah!

Gwyn Williams says that Jefferson Lab, where he worked after 21 years at BNL, periodically sends phishing emails to test the vulnerability of its own employees. [Editor's note: BNL does this, too.] Williams got one in February 2026. It appeared to come from LinkedIn. "It was the email address that it came from that made me suspicious," he said.

When Williams reported it to the service desk at Jefferson Lab, he got a thank you and an explanation: "This was a test conducted by the Cyber Security department here at Jefferson Lab. This email is a phishing email. A phishing email is a type of online scam where people impersonate legitimate people or organizations in order to steal sensitive information from others. These types of scams are a major threat in today's world, not only to individuals, but organizations as well. To decrease the chances of these types of threats getting into our organization, we conduct these phishing scams internally. Our end goal is to have an educated staff that can differentiate between a legitimate email from a non-legitimate email."

Yousef Makdisi gets bogus emails from participants at OLLI, the Osher Lifelong Learning Institute at Stony Brook University. "It started with one person who led a popular session. But the request was odd, so I deleted it without clicking on the offered venue." Then he realized that the sender's email address was coming from New Zealand.

"With my Mac and my mail from Optimum online, I realized that if one clicks on the triangle next to the name, you can block the sender," said Makdisi. "I usually block them, but it probably does not help as the scammers set new addresses." He also deletes them from the junk folder.

Makdisi advises:

- Look at the sender's address and make sure it is legitimate and not from outside the U.S.

(continued on next page)

- If only the sender's name is shown, click on the "v" next to the name to see the address.
- If you wish, block the sender.

Advice from government agencies

The FBI investigates financial scams targeting seniors, including investment scams, technical/customer support schemes, and romance scams. Seniors are often targeted because they tend to be trusting and polite. Plus, seniors usually have financial savings, own a home and have good credit, making them attractive to scammers.

Says the FBI, you can take simple steps to protect yourself and your information:

- Search online for the contact information (name, phone number, email, addresses) of any unknown source that reaches out to you. Others have likely posted information online about businesses and individuals attempting to run scams.
- Resist the pressure to act quickly. Scammers create a sense of urgency to lure victims into immediate action.
- Be cautious of unsolicited phone calls, mailings, and door-to-door service offers.
- Never give or send to unverified people or businesses any personally identifiable information.
- Take precautionary measures to protect your identity should a criminal gain access to your device or account. Immediately contact your financial institutions to place protections on your accounts and monitor for suspicious activity.

The United States Postal Service advises against sending paper checks through the mail because they are easily intercepted, copied, and used to drain your account. They also reveal critical information like your bank account, routing numbers, and personal details like your name and address.

Frank Scheifele may be newly retired but he's been using bank checks for years through his credit union. "Never had an issue," he says. Most credit unions and banks provide online bill pay. The service is free. It's also more secure because it does not expose your account information.

If you must use a personal check, always take your mail directly to the post office to avoid having checks stolen from mailboxes and blue USPS boxes.

Switching from paper checks to digital payments is safer. But the digital world has other risks.

AI scams on the rise

The 2026 March/April AARP Bulletin had a special section on fraud, including AI scams, which

are on the rise. Artificial intelligence is used to manipulate a video, photo or audio recording that seems real. Called deepfakes – "deep" for machine learning – they are used to impersonate family members, officials or celebrities to steal money or information.

Released in April 2026, the FBI's 2025 Internet Crime Report notes that cyber-enabled crimes defrauded Americans of nearly \$21 billion, with cryptocurrency and artificial intelligence-related complaints among the costliest.

While you can't trust your eyes and ears anymore, you can outwit AI with some basic advice from many sources: Pause and reflect before acting. And be skeptical of an offer that sounds too good to be true.

– Mona S. Rowe, msrowe.hi@gmail.com

“Cyber-enabled crimes defrauded Americans of nearly \$21 billion, with cryptocurrency and artificial intelligence-related complaints among the costliest.”

– FBI press release, April 6, 2026

Renew BREA Membership

Membership expires on December 31 of every year no matter when you paid your dues (which are requested by January 31 of the following year). To stay on BREA’s mailing list, complete the form below and mail it to me along with your payment. Include your email address so BREA can send you timely information.

If you have questions or if your contact information has changed, send me an email at bettyelder81@gmail.com.

PLEASE PRINT

Last name: _____ First name: _____ MI: _____

Street: _____ City: _____ Zip+4: _____

Phone: _____ Email: _____

Membership type:
 annual (\$10) 5 years (\$40) Life (\$95)

Dues cover year(s) _____

Date: _____ Check amount: _____

MAKE CHECK OUT TO BREA

I want to receive BREA News by mail via the U.S. Post Office.

I want to receive BREA News by email only. Do not mail it to me via the U.S. Post Office.

Mail form and check to:
 Betty Elder, Membership Chair
 215 River Drive
 Moriches, NY 11955

– Betty Elder, Membership Chair
bettyelder81@gmail.com

In Memoriam

We deeply regret to inform you of the passing of the following retirees.

Andrew Feldman, 80, March 10, 2026

Denis Donahue, 81, April 7, 2026

More information may be found at BREA’s website: <https://bera.bnl.gov/brea/>. To post an obituary for a deceased BNL employee or retiree, email information to msrowe.hi@gmail.com or mail it to BREA (see panel below for address).

President’s Message (cont’d from p. 1)

Springtime has finally arrived on Long Island. BREA intends to have an in-person regular meeting at BNL, which will also be available to remote members via Zoom. Final planning depends on the availability of BNL facilities and support.

Our next meeting is Tuesday, May 12, 2026, 1 p.m. If that one is a hybrid meeting – on site and via Zoom – we will call your attention to that in the email invitation/agenda sent to you in the first week of May. Note that the BNL-originated meeting Zoom.gov login process will differ from the Zoom-only meetings. Contact an officer using email information in this newsletter if you have questions.

Best wishes to all our members. We hope to see you at our BREA meetings.

– Arnie Moodenbaugh, moodenba@optonline.net

Brookhaven Retired Employees Association

BREA c/o BERA
 Brookhaven National Laboratory
 Bldg. 400 Brookhaven Avenue
 Upton, NY 11973

Phone: (631) 344-5090
 Email: BREA@bnl.gov
 Web: <https://bera.bnl.gov/brea/>

