FRESNO COUNTY EMPLOYEES' RETIREMENT ASSOCIATION

The Retirement View

VOLUME 8, ISSUE 3 SUMMER 2015

INSIDE THIS ISSUE:

"Security Matters" by your Retirement Administrator	1-2
Survivor Checklist: Ensure Loved Ones Are Prepared	2
Important Notice: Office Staff Shortage	3
New Retiree Payroll Deduction	3
Calendar	3
Payment Schedule	3
Live Audio Broadcast	3
Board members	3
Meet Staff	4
Contribution Rates 2015-2016	Insert

"Security Matters" by your Retirement Administrator

I believe that we all deserve a secure retirement. That is why I love this job. That is also why I am writing on the subject of data security. I would like to focus on electronic data security, which involves the protection of our financial and personal data. It is difficult for us, as individuals, to protect against geopolitical threats, but there is a lot we can do to protect against cyber fraud.

The Internet is not new anymore, but Internet technologies utilized by criminals are evolving all the time, which is why I would like to provide you with information on some of the latest threats, the latest protections, and a refresher on tried and true practices for better electronic data security. It is not the end of the world, but Internet and data security are important and there is a lot that you can do.

The weakest link in our chain of security is ourselves! Technology is evolving and we need to stay current. Every institution you interact with likely has some of your personal data, and they are even more likely targets for a data attack than individuals are. You might be wondering how secure your data is with FCERA. First, we are not as large a target as one might expect. There are many bigger fish in the sea with records on tens of thousands to millions of individuals and our data is not as valuable as other's. We do not have credit card information, which is far more attractive to thieves. And while social security numbers and birthdates are of value, many other sources exist that are more expansive, and are higher value targets. Our data is valuable to us, though, and I would like to assure you that we either meet or exceed current security standards (without going into the details).

Now for the threats, protective measures, and refresher

1. Weak Passwords – Even after several years of computing, folks still use "12345678" or "password" or worse. Strong passwords are far more secure, such as "!W!$hUWe11" (not that I am using this one, but you get the idea). Here are a few principles for creating strong passwords and keeping them safe:
   - The longer the password, the tougher it is to crack. Use at least 10 characters; 12 is ideal for most home users.
   - Mix letters, numbers, and special characters. Try to be unpredictable – don't use your name, birthdate, or common words.
   - Keep your passwords in a secure place, out of plain sight.

(Continued on Page 2)

"Security Matters" by your Retirement Administrator—Cont'd

- Don't use the same password for many accounts. If it's stolen from you – or from one of the companies with which you do business – it can be used to take over all your accounts. If you must use the same passwords, please consider at least a different, stronger, one for your email, making it harder for criminals to change others via online password resets.
- Don't share passwords on the phone, in texts or email. Legitimate companies will not send you messages asking for your password. If you get such a message, it's probably a scam.

2. Public Wifi (often free and not password protected) – With the advent of portable hot spots (wireless access) criminals are pretending to be a proprietor's free Wifi in order to steal your personal information. For example, the IRS does not provide free Wifi, so do not connect to "FreeIRSwifi" while you are there. Restaurants, coffee shops, airports, and other places where Wifi is commonly expected are potential danger zones. Experts say to use your mobile data instead, which is currently more secure, especially for online banking, email and other applications that pass data over the Internet. The latest advice is to turn off your Wifi (and blue tooth) any time you are away from your home or office and you do not need them. Criminals are using software to trick mobile phones into connecting to fictitious networks.
3. Phishing (fishing for an email reply with personal information or link click from you to malware) – the IRS does not email investigation inquiries, so do not answer them. For example, I have been told that my bank password, or email password, needs to be updated and have been given a link. I always go to the website separately or even call the bank first in order to verify. I recommend the same. Phishers are becoming convincing. (Continued on Insert)

Survivor Checklist: Ensure Loved Ones Are Prepared

Dealing with the death of a loved one may leave families overwhelmed and confused on all the tasks to be completed. Upon the death of a FCERA benefit recipient certain benefits may be payable to a surviving spouse, domestic partner, or designated beneficiaries; FCERA has created a checklist to assist loved ones through this difficult time.

- ☐ Step 1: Notify FCERA of the benefit recipient's death
- ☐ Step 2: Submit required documents
  - Death Certificate
  - Birth Certificate of Beneficiary to receive continuance
  - Marriage Certificate (if applicable)
- ☐ Step 3: Receive benefit payment(s)*

This checklist is intended to be informational and may not contain definitive information on matters of immediate concern upon death.

* Benefit processing time may vary according to how soon FCERA receives all the documents.

NOTE: The community property laws of the State of California may supersede the rights of designated beneficiaries.

"Security Matters" by your Retirement Administrator - Cont'd

4. Website or Email Links to Malware and Viruses (bad marketing software or data breaching software, and destructive software, respectively) – bad email links are threats in clever phishing attempts. They are common in chain emails and other informal email appearing to be sent from a friend. Most websites are reputable. Be especially careful with unreputable websites.
5. Outdated virus protection software– If your virus protection software is current, and you accidentally click a bad link in an email or on a website, a warning will likely pop up protecting you. If you get a warning, do not ignore it. If you get a warning online that asks you to install software in order to clean a detected threat, that is likely a virus, your installed software will not ask to install software, but might ask for an update.
6. Malware Embedded in "Freeware" (software payloads) – A legitimate form of software is freeware/shareware where the developers do not charge a fee to install and use it. Most software in the beginning was the benevolent creator's intent to share his or her good work. Criminals got into the act including malicious software, often creating targeted ads or sending out mass emails behind the scene (ergo the odd emails you might occasionally receive from a friend, mentioned under bullet 3). An example of a payload is one where you think you are installing a free wallpaper slideshow program, and you do get a wonderful slideshow program, but you also start to get Canadian Viagra adds every time you surf the Internet. Download with caution. Ensure that any software you are downloading is reputable and from a reputable source. If the download is free, ensure that the site can be trusted. Even reputable software sources such as Java or Adobe Flash, come with payloads. Pay particular attention when installing the needed updates, and uncheck the additional software, such as McAfee virus scanner or other search toolbars, unless you want them. They use the additional software as a source of revenue for themselves, but it could be a headache for you.
7. Embedded USB Malware and Viruses (hardware payloads) – A late breaking threat is the embedding of malware and viruses on the free USB drives you get from various conferences and other venues free. While it would be a stretch for an actual vendor to knowingly put a virus on the USB drives for a trade show, criminals could leave counterfeit ones lying around or pass them out to unsuspecting bystanders and not be associated with any vendor at a tradeshow. Even better, only buy reputable brands from reputable sellers, avoiding the generic, deep discount, brands offered as sale or holiday items.
8. Unprotected Home Networks – While routers in the beginning required personal action to password protect (and most of us did not take that action because it was a hassle) they now come with password protection as a default, less hassle. Unfortunately, they still come with a standard login ("admin") and password ("password") in order to make changes. Pranksters can lock you out of your own network. Thieves can monitor it for any valuable data.

(Continued on Page 2 Insert)

"Security Matters" by your Retirement Administrator - Cont'd

9. General security tips
   - When using a shared computer, always select "No" when prompted by the computer to remember your password for the next time you visit.
   - Avoid providing personal details, such as your date of birth if you use social networking, dating sites, or applications, such as Facebook, MySpace, Match, Tinder, or Instagram.
   - Always log off any websites that you are using before leaving your computer.
   - Always log off online banking sites before visiting any other websites.
   - When shopping online do not send your credit card details to retailers by email.
   - Never disclose your PIN at any time including when shopping online or by phone.
   - Consider changing your passwords at least every 60 to 90 days for your most critical accounts (like email and online banking), if not all your accounts. This is because criminals might obtain your passwords during a company data breach, but not be able to get through all of them for some time. Changing your passwords regularly decreases the chance a stale (old) stolen password will work.

In closing, the good news is that there are far more good people in the world than bad. Odds are in your favor that you will not have any problems as long as you take basic steps to be careful. Lastly, as long as you are a little more vigilant than the careless, unprotected citizen, they will be the target, not you. For more information on electronic security, please see your local library or Google.

Contribution Rates 2015-2016

New retirement rates are effective for the first paycheck issued in July 2015. The average employee retirement contribution rate for Fiscal Year 2015-2016 increased in all tiers.

	General Member					Safety Member			
	Tier 1	**Tier 2**	**Tier 3**	**Tier 4**	**Tier 5**	**Tier 1**	**Tier 2**	**Tier 4**	**Tier 5**
FY 2015-2016 (Current Fiscal Year)	**9.73%**	**6.98%**	**7.74%**	**6.68%**	**7.02%**	**12.52%**	**11.06%**	**9.83%**	**12.51%**
FY 2014-2015 (Last Fiscal Year)	9.61%	6.87%	7.56%	6.51%	6.96%	12.36%	10.93%	9.60%	11.96%

FCERA has placed a "retirement contribution calculator" on the website at www.fcera.org to aid you in estimating the impact that the new rates will have on your retirement contribution. Please note that County employees will need to add both retirement contribution deduction amounts reported on your check stub to compare the new total contribution deduction to your current total contribution deduction.

Important Notice: Office Staff Shortage

FCERA is experiencing a severe staffing shortage. On June 3rd, the FCERA Board was updated on the situation and agreed to implement a "critical plan of action".

- FCERA will be open to the public from 9 to noon and 1 to 4. Should you call during the non-operational hours, you may leave a message on the answering machine or should you come to the office during the non-operational hours, a drop box will be available for you to submit forms/paperwork.
- Phone calls will be routed to voice mail, with a return phone call within 48 hours.
- FCERA staff will only be able to meet with members that have an appointment.
- Email requests will be responded to within five (5) business days.
- Service Credit Purchase calculations will be limited to those members who are retiring.

We encourage you to use the FCERA website, www.fcera.org, for benefit calculations and general questions. Look to the website for more detail on the staff shortage.

It is FCERA's hope that with your patience and understanding of the situation, we can work together; and that this situation is temporary and short-term. It is our goal to return to normal, offering exceptional customer service as soon as possible.

New Retiree Payroll Deduction

Exciting news! The Board of Retirement has approved the authorization for retiree payroll deductions for premiums for additional benefit items available through SACRS and REFCO. Information will be mailed when it becomes available. Continue looking at the FCERA website and newsletters for updates!

Calendar

Next Regular Board Meeting:
August 5, 2015
August 19, 2015
September 2, 2015
September 16, 2015
Location:
FCERA Boardroom
1111 H Street
Fresno, California 93721
Time: 8:30 A.M.

Pension Payroll Payment Schedule

Friday, July 31, 2015
Monday, August 31, 2015
Wednesday, September 30, 2015

Live Audio Broadcast

FCERA broadcasts all board meetings live via streaming audio. Visit www.fcera.org for more information.

Board of Retirement

- Steven J. Jolly, Chair
- Dr. Rod Coburn, III, Vice Chair
- Laura P. Basua
- Gregory J. Baxter
- Vicki Crow
- Paul Dictos, CPA
- Robert Dowell
- Eulalio Gomez
- Mary Ann Rogozinski, Alternate

Fresno County Employees'
Retirement Association

1111 H. Street
Fresno, CA 93721
Phone: 559-457-0681
Fax: 559-457-0318
Internet: www.fcera.org
Intranet: http://www2.co.fresno.ca.us/9200/default.htm
Email: FCERAwebmail@co.fresno.ca.us

Meet FCERA Staff: Jared Wong-Account Clerk

I began my employment with FCERA in February 2015 as an Account Clerk II. The staff has been very welcoming and helpful during my transition. After graduating from Fresno State with a degree in Accounting, I moved to Orlando, FL to take an internship with The Walt Disney Company. Through my time there I learned a lot about guest services, management, marketing, teamwork, and leadership. Most of these tools I still use daily. Prior to joining FCERA I worked in public accounting for over 3 years and I am also actively pursuing my CPA license.

On my free time I like to spend time with my friends and family. I like to travel to different places like Orlando, Anaheim, or the bay area. I also love being out on the golf course, running half marathons, and keeping up with current technology.