CommunityTimes

October 25, 2012

Manage Your Information from Home with 'myHR'

All Community Transit employees have a new benefit – myHR!

With this new webpage you can review your pay stub, benefits, leave balances, manage your employee contact information and more from work or home. During Open Enrollment, Nov. 1-15, you will now be able to update your benefit choices online.

Much of the information on myHR has been available through PeopleSoft, but not everyone had a login and it was not easy to find. Now, Human Resources and Information Technology have joined to create a simple-to-use page that you can access at your convenience. This is also the first time employees can access HR information from home!

Visit myHR *at work* by going to the company intranet and clicking the "myHR" link.

Visit myHR *at home* by typing "myHR.commtrans.org" into your Internet browser's URL bar.

Log in using the same network user ID and password that you use to login every day at work. If you do not have an ID, contact the Help Desk at x6100 to get one.

This year's Open Enrollment will be a breeze with myHR. Employees can review current benefits and make their selection with a few clicks of a mouse. People who make benefit changes may get a follow-up form at work to fill out. Of course, you can still do things the *old-fashioned way* and fill out the Open Enrollment package you receive at work.

Please remember that when you access myHR you are displaying your personal information. Community Transit has taken steps to make this connection secure in several ways:

- No Social Security numbers are shown. If you need to update a SSN, contact HR directly.
- The myHR webpage is encrypted; information will be garbled if intercepted by a third party.
- myHR will automatically time out if there is no activity for 10 minutes.
- Employees must update their password every 90 days.

You can do your part to maintain security of your information by:

- Never sharing your Community Transit network password.
- Only access myHR or other sensitive websites through a secure network. If you have a wireless network at home, be sure it is password-protected. Do not log into this page through a public wi-fi network (like at Starbucks or an airport).
- Other tips for maintaining cybersecurity are included later in this newsletter.

Open Enrollment is Nearly Here!

Open Enrollment for your 2013 benefits starts November 1 and runs through 5 p.m. on November 15. *Note, for employees whose medical, dental and vision coverage is provided through the IAM, your open enrollment for those benefits happens in June of every year.*

There are other shared benefits that all employees need to consider, so everyone should review the information in the benefit packets that will be delivered by November 1. Human Resources representatives are available to answer any questions throughout Open Enrollment.

What you can expect:

- Changes to the PEBB medical plans are minimal. Check your packet for details.
- For administrative employees selecting one of the CDHP (high deductible) plans, there will be no premium contributions in 2013. Administrative employees selecting one of the other plans will contribute 5 percent towards their medical premiums.
- Premium deductions for 2013 will begin on the first December paycheck in 2012. For months with three paychecks, the third paycheck will not have a premium deduction.

Events:

- Community Transit Benefit Fair – 9 a.m. to 3 p.m., November 12, MCOB Great Hall.
- ICMA Representative onsite - November 12. Call Mary Lowery at x.2382 for appointments.

What is Our New Short-Term Shared Outcome?

The answer to this and other nagging questions can be learned at Food for Thought employee meetings. Join Joyce Eleanor and department directors as they update the company on the 2013 budget, Transit Technologies, 2013 service and fare change, and the United Way campaign.

Light snacks and refreshments are served. Remaining meetings are as follows:

- **Friday, Oct. 26, 9:30-10:30 a.m. – MCOB Drivers Lounge**
- **Monday, Oct. 29, 1-2 p.m. – KPOB Traning Conference Room**
- **Wednesday, Oct. 31, 9-10 a.m. – MCOB Drivers Lounge**

Live United: Fundraising Drive Ends with a Spin, Oct. 31

For many years, Community Transit employees have opened their hearts and wallets in support of the United Way of Snohomish County. So far this year, we have collected nearly $30,000 in pledges!

Our own Joyce Eleanor leads the county-wide campaign as the United Way Campaign Chair for 2012. She has chosen the theme Get On Board, which reflects our transit roots and shows our commitment to helping others throughout our community.

We're planning a fun event in the Great Hallway, from 10 a.m. to 3 p.m. October 31 that can't be missed! Come enjoy fresh, hot kettle corn, bid on an item in the silent auction and spin the wheel for a chance at a prize. To be eligible to spin the wheel, all you need to do is turn in your pledge form.

We are also giving away a Grand Prize valued at $250. For every $100 that you pledge, you will be entered in the Grand Prize drawing.

All prizes have been donated to give away to Community Transit employees. More prizes are coming in each day. Here's a partial list:

- $250 Visa card
- Starbucks gift cards
- Pizza gift cards
- Dinner-for-two at local restaurants
- Leaf blower
- Leather bomber jacket
- Model Boeing plane

Protect Your Identity Online – Tips for Cyber Security

Submitted by Ann Martin & Dave Tovrea, IT

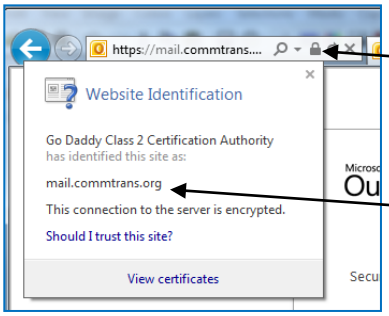
New security vulnerabilities are constantly arising. Perhaps most concerning, hackers can steal your personal information anywhere that it is made digital—on your computer, smartphone or tablet, at the checkout counter, the gas pump, and even at the doctor's office. While no strategy can ensure this absolutely will not happen, there are a number of things that you can do to decrease your risk:

- Keep anti-virus and anti-spyware software updated. Because new viruses are emerging daily, it is essential to configure your anti-virus software to update daily.

- Configure your computer to check for new patches automatically, at least weekly. Patches often fix security holes that attackers can use to gain access to or control of your computer.

- Use a firewall. Firewalls may be part of the operating system (Windows), part of the antiviral software (Norton, McAfee, AVG, etc.), or commercial hardware or software.

- When accessing sites that contain your personal information (financial or otherwise), make sure the site is the site it's supposed to be. This can generally be done by clicking on the "lock" icon:



Note the 'lock' icon. When you click on it, the website identification information should appear.

The last two parts of the name that shows on the certificate should match the site you expected to see (in this case, commtrans.org).

- Make sure any online credit card charges are handled through a secure site or in an encrypted mode. You'll know you're on a secure site if the web page on which you conduct your transaction begins with "https" instead of the usual "http" and the lock icon should be present.

- Always log out of websites that contains your personal information, including banking and employer benefit or retirement websites, any time you step away from your computer.

- Delete suspicious emails without replying. When you reply to messages, you are confirming to the sender that you are at a valid email address that could be targeted for future attacks.

- If you aren't sure if an email is legitimate, call the company. Don't use the phone number in the email, confirm the validity by calling a phone number from a recent statement or other source.

- Do not download ANY files or click on ANY links, including those being sent by people you know, unless you are expecting it. Many times viruses are transmitted by using email address books of virus-infected computers. These messages will appear to originate from that person (often times your friend or relative), but are being sent by that person unknowingly. When you click on the link or open the attachment, your computer becomes infected too.

- Use "strong" passwords for all of your accounts. Strong passwords have a combination of letters, numbers, special characters and should be seven or more characters long. Also:
  - Change your passwords often, ideally every 60 to 90 days.
  - Each account should have its own unique password since that prevents an attacker from gaining access to multiple accounts if they learn a single password.
  - Avoid using obvious words and numbers, such as birthdates and names.
  - If you have too many passwords to remember easily, consider using a password manager program like KeePass.
  - Never store your login and password information in clearly visible places; do not share your logon information with other users.

- When using a wireless network at a coffee shop, motel, airport or similar public location, ask the staff for the name of the wireless network you should use and ONLY use that network. Do not assume that because a wireless network is present that it is safe to use.

- Do not access your bank account or enter your social security number on your unprotected smartphone or tablet. If you plan to use your smartphone or tablet to access your personal information, install anti-virus software to protect these devices as well.

- Only shop on websites that offer a privacy policy. Read the privacy policy on any website to ensure your information is secure. Know how your personal information will be handled.

- Review your bank and credit card statements frequently online and make sure all the transactions are legitimate.

- If you have a laptop, do not leave it unattended. If you are storing your laptop, keep it locked up, where it is not visible to others.

- If you store data on portable media such as a thumb (flash) drive, make sure the data is encrypted.

- Remember, anything you post on social network sites (Facebook, Twitter, etc.) potentially could be viewed by anyone, including your employer or the burglar waiting for you to go on vacation. Be aware of your privacy settings, keep your profile private and avoid posting information in public areas that should not be public knowledge.

Pool Table Available to Non-Profit Organizations

The Employee Association is looking for non-profit organization in the community that would be willing to give our ping pong table a new home. We would like to make sure that they have room for it and would utilize it. If you know of such a group, please have them contact Pam Muellenbach at pam.muellenbach@commtrans.org or (425) 348-2354.

Marijuana is a Prohibited Substance – Agency Policy

Submitted by Human Resources

Community Transit's Drug and Alcohol policy declares marijuana as a prohibited substance. Employees who test positive for any prohibited substance will be terminated.

Employees should be aware that being on company property (not just for work) while having a prohibited substance in your system will result in immediate termination.

Community Transit's interest is in ensuring everyone's safety and being able to trust that folks around you are safe, too.

"Vendors wanted for the
Annual Holiday Bazaar!"

Thursday, November 29th &
Friday, November 30th

Full table $40 Half table $20

Reserve Your Table Today!

(thru 10/30 only) Pam Muellenbach ext. 2354

(after 10/30) Andrea Carter ext. 2330

or email: employee.association@commtrans.org

Employee Association for Community Transit
Activities • Benefits • Morale