BEC February NEWSLETTER
The Breakfast Exchange Club of Billings

EXCHANGE
BREAKFAST EXCHANGE CLUB OF BILLINGS, MT

February—Be Aware

Common Tech Scams

Malware

You can download programs on the Internet to look at pictures, play games, listen to music, and enjoy other activities. But, beware of dangerous downloads that may result in serious computer problems and expenses that you did not anticipate.

- **Some downloads contain viruses.** These could wipe out your computer files. Get a good virus software program and regularly update it to protect your computer.
- **You may be downloading a dialer program without realizing it.** This would enable it to "highjack" your modem and connect it to a foreign telephone number, resulting in expensive phone charges. Some programs turn off the volume so you can't hear the dialing take place.
- **Don't download programs from Web sites you don't know and trust.** Make sure that everyone in your household or business checks with you first before downloading programs.
- **Be cautious about emails offering information or entertainment services.** Many unsolicited emails are fraudulent and sometimes even opening the email or clicking on an attached link will send a virus through your computer.
- **Read the user agreement carefully.** There may be important information buried in the agreement about costs or other aspects of the program.
- **Supervise children when they're surfing the Internet.** Lured by promises of fun, children may ignore the user agreement or other warnings. Family members who are worried about children surfing the internet should take advantage of the ability to block Web sites and programs.
- **Limit the people who know the password needed to go online on your computer.** This is an easy way to keep friends, babysitters, and others from downloading dangerous programs onto your system.

Continued on page 2...

Volume 3, Issue 8

February 2020

In this issue:

February Quote: "It's not enough to have lived. We should be determined to live for something. May I suggest that it be creating joy for others, sharing what we have for the betterment of personkind, bringing hope to the lost and love to the lonely." — Leo Buscaglia

Club President:

Rene Critelli

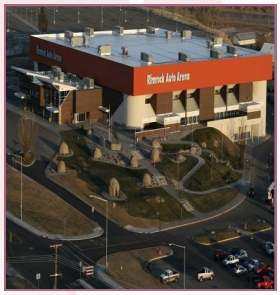
EXCHANGE
BREAKFAST EXCHANGE CLUB OF BILLINGS, MT

February Volunteer Opportunities:

February 22—Monster Trucks

Future Volunteer Opportunities:

April 17-19—PBR
April 26—Cher
May 15—In This Moment
June 13—Food Truck Battle
June 19—Toby Keith



Come weekly at 7:00 a.m. on Friday to the Yellowstone Room and get to know your fellow Exchangites!

2018 BEST CLUB BULLETIN
Exchange Club
75 or more members

- **Increase the amount of time a site is kept in your browser history file.** Usually a site is erased from the history folder after 20 days, but it may take longer for you to discover that you have been victimized. Increase the time to 45 days. Your browser's help folder can provide instructions on how to do this.

- **Install monitoring software on your system.** This software keeps a log of all programs installed on your computer and sites visited on the Internet. It will help you enforce the "no downloading" and "no unsupervised surfing" rules and track down any problems. Monitoring software also allows you to sweep your computer for any viruses using the instructed program.

- **Look at your phone bill carefully before you pay it.** If you find charges for foreign phone calls you did not knowingly make, your long distance company may agree to remove them or adjust the amount. Your service could be shut off for refusal to pay unless you can work something out.

Tech Support Scams

A fraudster, claiming to work for a well-known technology company like Microsoft or Norton, contacts you claiming that viruses have been detected on your computer. The fake tech representative alleges they can remotely remove the virus for a fee (typically between $100-400). Think twice before paying up or allow them access to your computer.

Sometimes the hacker charges a consumer to download harmless programs that are available for free online to demonstrate the alleged virus. Other times, they install tracking software that gives the fraudster access to personal information on the computer.

Estimates of the scope of this scam vary widely. For example, Microsoft reported that the average victim lost $875 and had to pay $1,700 in repair bills. The Federal Trade Commission (FTC) said it had received more than 40,000 complaints about this scam when it initiated a crackdown in October 2012 and an official with the FTC's consumer protection bureau said he thought the number of victims was probably "substantially higher."

Although scams of this sort started in 2008, it has become far more common in the last couple of years, gaining attention from media organizations across the world. The companies that are affected have also noticed, warning their customers and offering tips on how to spot and avoid the scam. PayPal and other payment companies have helped by shutting down the accounts of known fraudsters.

Despite government action to identify and stop scam artists running these schemes, copycats continue to defraud consumers. Consumers should use the following precautions to minimize the risk of falling victim:

- **Do not assume that the person contacting you is legitimately working for the company they say they are.** Know that legitimate companies will not call you without solicitation and tell you that you must pay for tech support.
- **Reach out to the tech company yourself.** Find a legitimate phone number for the company and ask them whether a representative contacted you.

Continued on page 3...

- **Don't allow remote access to an unauthorized stranger.** Never allow someone to take remote control of your computer unless you are certain that they are actually representing a legitimate company.
- **Don't share personal information.** Do not disclose sensitive financial information such as passwords, credit card, or bank account routing numbers over the phone.
- **Keep a record of your charges.** When buying things over the Internet or phone, use a credit card or a debit card so that you can better dispute fraudulent charges.

If you believe that you are the victim of a tech support scam, please take the following actions:

- File a complaint with Fraud.org so they can help others avoid falling victim;
- Call your credit card company and ask to have the charges reversed;
- Check your bank and credit card statements for inaccuracies. If you find any, ask that those charges be reversed, too;
- Contact the major credit-reporting agencies (Equifax, Experian, and TransUnion) and notify them of the potential for fraud on your account; and delete the tracking software from your computer.

Unwanted Software

Unwanted software are programs that are downloaded—often unknowingly—that can cause serious problems for computer users. Examples of unwanted software are spyware, adware, and a host of other programs. Sometimes unwanted software comes hidden along with a program that the user actually intended to download.
Tips on protecting yourself from unwanted software:

- **Get your software directly from the source.** When you're looking for a new program, look for the publisher's website first. Software download repositories may bundle in unwanted software with legitimate downloads.
- **Avoid clicking on pop-ups or banner ads that warn you of slow performance on your computer.** This is often a ruse to lead you to websites that host unwanted software.
- **Make sure everything is up-to-date.** To best protect yourself, repeatedly update your browser and operating systems; older systems are more susceptible to being infected by malware.
- **Routinely scan your computer.** Use antivirus software to regularly scan your computer for programs that you don't recognize.
- **Pay attention when installing new software.** When downloading programs and extensions, pay attention to the fine print details. In particular, be on the lookout for pre-checked boxes that offer to install things like toolbars or other software in addition to the software you were looking for.
- **Heed your browser's warnings.** Most major Web browsers now have functionality built-in that will warn you when you are about to enter an unsafe website. Chances are that if your browser is telling you to not visit a certain website or download a particular program, you're better off steering clear.

Despite our best efforts, it's still possible to inadvertently install unwanted software. Once it happens, there are several steps you can take:

- **Ensure that the latest versions of your browser and operating system are installed.** The best way to defend yourself against unwanted software is to ensure that your Internet browser (Safari, Firefox, Chrome, Edge, etc.) and operating system (Windows, OSX, Linux, etc.) are up-to-date.
- **Run a security scan using a reputable antivirus removal tool.** While this software isn't perfect, an antivirus tool can help detect and remove unwanted software. If you suspect you have unwanted software on your computer, make sure your antivirus tool is up-to-date and then run a full scan. The antivirus may help to detect and remove such software.

Continued on page 4...

- **If all else fails, format and reinstall.** In extreme cases, unwanted software may be so persistent that it disables operating system or browser updates and resists antivirus removal. If it comes to that, it may become necessary to format your hard drive and reinstall your operating system and Internet browser. *Before* you do this however, be sure to create backups of important files (like photos, videos, documents). WARNING: This may be a time-consuming process and beyond the skill of some users. If you don't feel comfortable doing so, you may need to look for outside computer help from your local electronics store or computer manufacturer.

Phishing

In a scheme called "phishing," ID thieves trick people into providing their Social Security numbers, financial account numbers, PIN numbers, mothers' maiden names, and other personal information by pretending to be someone they're not.

- **Watch out for "phishy" emails.** The most common form of phishing is emails pretending to be from a legitimate retailer, bank, organization, or government agency. The sender asks to "confirm" your personal information for some made-up reason: your account is about to be closed, an order for something has been placed in your name, or your information has been lost because of a computer problem. Another tactic phishers use is to say they're from the fraud departments of well-known companies and ask to verify your information because they suspect you may be a victim of identity theft! In one case, a phisher claimed to be from a state lottery commission and requested people's banking information to deposit their "winnings" in their accounts.
- **Don't click on links within emails that ask for your personal information.** Fraudsters use these links to lure people to phony Web sites that looks just like the real sites of the company, organization, or agency they're impersonating. If you follow the instructions and enter your personal information on the Web site, you'll deliver it directly into the hands of identity thieves. To check whether the message is really from the company or agency, call it directly or go to its Web site (use a search engine to find it).
- **Beware of "pharming."** In this latest version of online ID theft, a virus or malicious program is secretly planted in your computer and hijacks your Web browser. When you type in the address of a legitimate Web site, you're taken to a fake copy of the site without realizing it. Any personal information you provide at the phony site, such as your password or account number, can be stolen and fraudulently used.
- **Never enter your personal information in a pop-up screen.** Sometimes a phisher will direct you to a real company's, organizations, or agency's Web site, but then an unauthorized pop-up screen created by the scammer will appear, with blanks in which to provide your personal information. If you fill it in, your information will go to the phisher. Legitimate companies, agencies and organizations don't ask for personal information via pop-up screens. Install pop-up blocking software to help prevent this type of phishing attack.

www.fraud.org

THE BREAKFAST EXCHANGE CLUB OF BILLINGS, MT

PO Box 2224
Billings, MT

www.breakfastexchangeclub.org

Exchange, America's Service Club, is a group of men and women working together to make our communities better places to live through programs of service in Americanism, Community Service, Youth Activities, and its national project, the Prevention of Child Abuse.

Looking for something to do and support community organizations at the same time?

- 1st—FREE Eating Healthy Grocery Store Tour (Albertsons 511 Central)
- 2nd—Froze Nose Biathlon
- 7th —Winter ArtWalk
- 14th—Valentine's Partner Yoga (Limber Tree)
- 15th—406 Resolute Runner 5k
- 15th—Big Brothers & Big Sisters Gala
- 15th—My Furry Valentine (YVAS Fundraiser @ Pub Station)
- 29th—Beach Blizzard Fundraiser

EXCHANGE
BREAKFAST EXCHANGE CLUB OF BILLINGS, MT

CAP Center Corner

The Importance of Family Mealtime

For many, family mealtime has been lost in our overscheduled lives. For many families, school, work schedules and extracurricular activities can make it difficult to find time to eat together and some go days or weeks without sitting down as a family to share a meal. However, family meals are important and should be considered part of our daily requirements.

Researchers have found that families who share meals together on a regular basis, whether it's breakfast, lunch or dinner reap many benefits.

- Family meals are more nutritious. A Harvard study found that families who eat together are twice as likely to eat their five servings of fruits and vegetables as families who don't eat together.
- Kids who eat family meals tend to eat a wider variety of foods and become less picky eaters.
- Family meals provide an opportunity for family members to come together, strengthen ties and build better relationships. They build a sense of belonging which leads to better self-esteem.
- Family meals offer parents a chance to be role models. They can set an example of healthy eating and polite table manners.
- Family meals help prevent obesity. Research shows that people tend to eat less during family meals because they eat more slowly, and talk more.
- Research shows that kids who eat family meals have a lower chance of engaging in high risk behaviors such as substance use and violence, and fewer psychological problems.

Tips for eating more meals together:

- Make family meals a priority in your household. Focus on the importance of being together as a family more than on making an elaborate meal.
- Start with small steps. Increase the number of family meals by one extra meal a week.
- As a family, plan a menu for the week and make a grocery list.
- Let the kids be involved. Let them help prepare food or set the table.
- Work as a family to clean up afterwards.
- Turn off the TV.

It's worth a try. More family mealtime could mean large rewards for your family.

https://www.fcconline.org/

EXCHANGE

BREAKFAST EXCHANGE CLUB OF BILLINGS, MT

Committee Happenings:

BECON Committee—Your February BECON Editor is Wayne Moller.

Food Truck Battle Committee—Committee has the date for June 13th. Working on securing bands and recipient/s of funds raised.

Freedom Shrine —Freedom Shrine rededication coming up at McKinley School.

Other Happenings:

District Convention—May 8th and 9th in Butte

National Convention—July 22nd—25th in Colorado Springs, CO

GET INVOLVED!

Committee Chairs—Please email your upcoming events to dinaharmon1212@gmail.com to be included in next months newsletter!

Interesting Valentine's Day Facts:

- On Valentine`s Day every year, there are at least 36 million heart shape boxes of chocolates sold.
- On average, men spend double the amount of money on Valentine`s Day gifts than women spend. The average amount a man spends is $130.
- There are enough candy hearts made each year to stretch from Valentine, Arizona to Rome, Italy, and back again. The number of these candy hearts produced is approximately 8 billion.
- There are approximately 50 million roses given on Valentine`s Day around the world.
- Women tend to buy approximately 85% of all the Valentine`s Day cards sold.
- Valentine`s Day is the second most popular day of the year for sending cards, second only to Christmas.
- There are approximately 1 billion Valentine`s Day cards exchanged every year in the U.S. alone.
- Approximately 27 percent of those who buy flowers on Valentine`s Day are women. The other 73% are men.
- The phrase to wear your heart on your sleeve has historical meaning. In the middle ages young people would draw the name of their valentine from a bowl. They had to wear the name on their sleeve for one week.
- Every Valentine`s Day, the Italian city of Verona receives approximately 1,000 letters that have been addressed to Juliet. This is where Romeo and Juliet, the young lovers in Shakespeare`s play, lived.
- The first Valentine`s Day candy box was invented by Richard Cadbury in the late 19th century. Shakespeare`s play, lived.
- On Valentine`s Day, 1876, Alexander Graham Bell applied for his telephone patent.
- Cupid is the son of Venus. Venus was the god of beauty and love.
- Approximately 15% of women send themselves flowers on Valentine`s Day.