Alan Amanda AnneK BarbaraCBetty J BillieB Bob H Bob M Brad W BrianD CarrieH Charles CherylM
Corey T CraigW Curt L Dan M Dana M DaniJ Dave H DawnT DeanaD DebbieH DebbieK DebbieR
DonnaG ElizabethErik L Faye O GingerB Greg C Gunnar Haris JamesWJan S Jean L JeanM JenniferO John K
Joy B Judy D JulieK Julie T Kal R Kasra Keith B Kent W KevinG Kori K Kris F KrissyH KristaN
KristaTKristalG Laurie LindaH LindaT LisaJ Mai MargaretteN MariaS Marilyn MarleneMarshall
MarySueMary S Michael NancyB Norma Pat S PattiM PhilR RebeccaK Renee RobB Roberta RonL
RuthC SharonFShawn ShelbyP ShelleyS StephH SteveH SueP Suzanne Todd G VeronicaS WilmaL

RE/MAX Equity Group
Portland Executive Office Business Meeting
Tuesday December 1, 2008 9:00am

Breakfast Sponsor: John Reinwald First American Title 503.319.3999

Haves and Wants: Tour Properties - New Listings - Buyer Looking For? - Great Deals!!

Equity Home Mortgage: Bob/Don

Office: **Congratulations Ruth Canutt** **Congratulations Bob Chiodo & Don McKay**

Need an end of the year business tune-up? Business planning, systems and results realignment? Set a FREE 1 hour appointment with Alan, business coach, counselor and confidant... ext 5194

Get signed up for Wednesday Dec 10 4:00pm – 7:00pm PE Office Conference Room
PE Office Christmas Party
Wine and Beer, Appetizers, Music, Silent Auction, Charity Gift Drop Off and FUN
Judged Dessert Contest with Prizes

Lunch and Learn Thursday: 12/04 e-cinchL
Lunch @ 11:30am 12/11 Old School Networking Scotte Perry Lawyer's Title
Class starts @ 12noon

EG Foundation: Shawn McDonald Office Project

Company: Recently Russ presented a $10,000 check from EG Foundation to Wounded Warrior Sentinels
Almost $100,000 raised into the foundation this year

Real Estate Business:

Return of the Predators

RMLS Issues NEW RULES! Status changes must be made within 72 hours. (not 4 bus days)
Private ID Change by December 10

Happy December Birthdays: **Amanda MacLaughlin 3rd, Mai Truong 4th, Craig Weatherford 7th, Krista Nicoli 11th, Kasra Shakerin 12th, Shelley Collins 12th, Donna Gardinier 16th, Charles Buck 17th, Lisa Jost 17th, Ron Lambert 21st, Kris Focht 25th, Shawn McDonald 27th,**

It's a great day to buy or sell real estate!

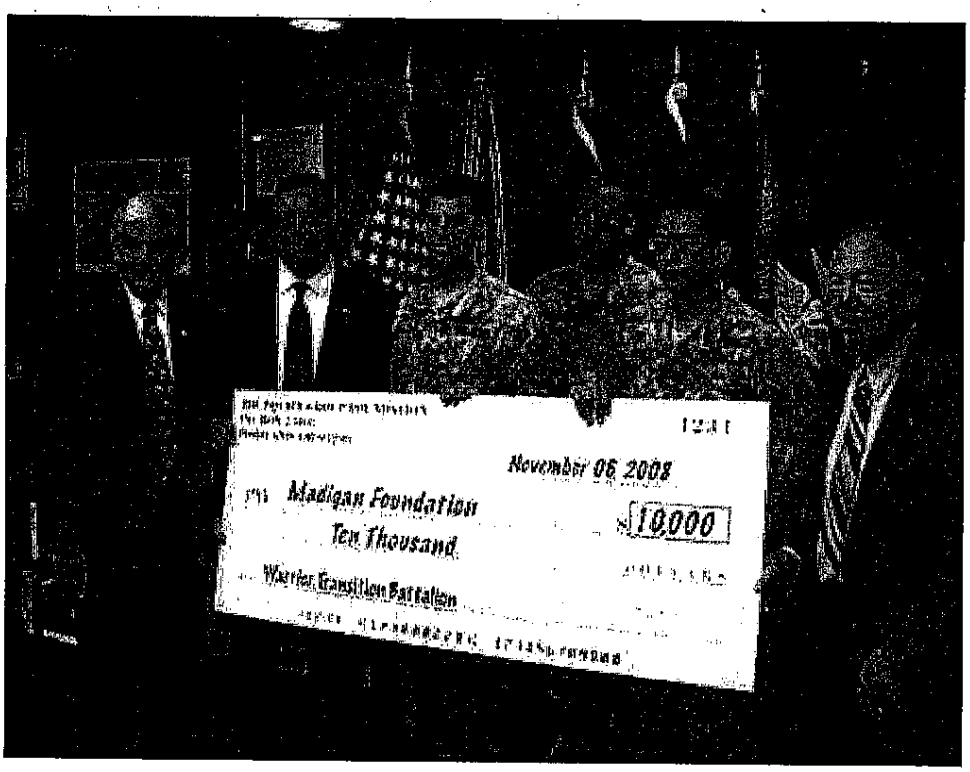
MLS#:	8107478	**Area:**	148	**Prop Cat:**	RES	**L/Price:**	$475,000
Address:	2015 SW WARWICK AVE 97225			**Unit #:**		**Map Coord:**	625D1
City:	Portland	**Yr Built:**	1962	**Bdrms:**	5	**Total Bath:**	3
Total SF:	3130	**L/Off:**	EQTY25	**Style:**	DAYRNCH,SPLIT	**Access. Y/N:**	
Agt Name:	Kori Koppen			**Contact#:**	503-495-5179	**Acres:**	0.2
Date:	12/2/2008			**Time:**	11 AM - 1 PM	**Food:**	Y
Remarks:	Easy to show - owners have moved due to relo. Great location just blocks to Cedar Park MS, Roxbury Park & Comm Cntr. Spacious floor plan, mature landscaping with greenhouse. Upper deck off living/dining rm - covered patio off fmly rm. New roof & gutters in '08 - move in ready!						
Directions:	Cedar Hills Blvd, E Berkshire, N Warwick OR Roxbury, Berkshire, Warwick						

MLS#:	8108036	**Area:**	151	**Prop Cat:**	RES	**L/Price:**	$775,000
Address:	5125 SW PROSPERITY PARK R 97062			**Unit #:**		**Map Coord:**	685J5
City:	Tualatin	**Yr Built:**	1935	**Bdrms:**	5	**Total Bath:**	5.1
Total SF:	6055	**L/Off:**	EQTY25	**Style:**	2STORY	**Access. Y/N:**	
Agt Name:	Julie Kumler			**Contact#:**	503-691-6393	**Acres:**	3.2
Date:	12/2/2008			**Time:**	11am-1:30pm	**Food:**	Y
Remarks:	FULL HOT LUNCH SERVED. GREAT GRAB BAGS FULL OF NICE STOCKING STUFFERS FOR EVERY REALTOR!! Country Living w/ contemporary twist.3.20 level acres. Nice open floor plan. FR w/ tons of built-ins & a Built-in 200 gal Aquarium. Sep. suite w/brm and bth in uppr wing of home. Office,Library,& More! Views, 28 X 40 pole barn + 2 car garg & 2 Stall horse barn w/tack rm & fenced pasture.						
Directions:	Borland Rd to Prosperity Park						

© RMLS™ 2008. ALL RIGHTS RESERVED. - INFORMATION NOT GUARANTEED AND SHOULD BE VERIFIED.

Alan Mehrwein

From: Russ Newcomer [RussN@equitygroup.com]
Sent: Wednesday, November 26, 2008 3:59 PM
To: all@equitygroup.com
Subject: Thank You For All Your Support
Attachments: image003.jpg; image001.jpg



To All Equity Group ~

Thanks for all you do!! 2008 has been an interesting year, forcing many of us to watch our dollars even more carefully.

In spite of these conditions you were able to generate nearly $100,000.00 so far for our foundation, of which $10,000.00 was earmarked for The Wounded Warrior Sentinels program.

Congrats to the many REALTORS® at RE/MAX Equity Group for your support.
You gave us the opportunity to present a $10,000.00 check for the benefit of The Wounded Warriors at Ft. Lewis. Tuesday at The Madigan Medical Facility in Washington.

This is a state of the art facility serving service men and women from all branches of the military and their families. I am happy to report that many of the available beds are now empty and that the number of returning wounded service people have been declining this year.

We have a lot to be thankful for including the service of these young men and women.

Thanks to all of you for the support of the many programs served by The Equity Foundation.

Have a great Thanksgiving and let's all plan to excel in 2009 so we can continue to give!!

Russ Newcomer

The New York Times
nytimes.com

PRINTER FRIENDLY FORMAT SPONSORED BY From Daddy

November 24, 2008

EDITORIAL

Return of the Predators

The demise of the subprime mortgage industry has been hard on predatory brokers, too. They feasted for years on bad loans until reality crashed down and the money ran out, and there they were: sharks without a frenzy.

Now they are circling again. Predators of every sort have regrouped and returned to their old ways, this time as loan-modification companies, inserting themselves between hard-strapped homeowners and banks, offering to work deals — for cash up front.

It's a high-pressure, high-volume business, advertising in the usual low-rent ways: talk-radio ads, Web come-ons, fliers on car windshields. The ads are full of glossy promises, like this one for a Long Island outfit: "Reduce your mortgage rate to as low as 4%. No refinancing — no closing costs. Reduce your monthly payment. Foreclosures, late pays/bad credit okay."

It'll cost you — in this case, 1 percent of your outstanding loan, half of it in advance.

There's often nothing illegal about this booming and largely unregulated business. Some shops are true scams, taking the money and running. But others are just immoral, profiting on fear and false hopes with expensive services that nonprofit organizations and government agencies offer for nothing.

Troubled homeowners know all about the relentlessness of the loan-rescue racket: it fills their mailboxes and sends salespeople to lurk on their doorsteps. Foreclosure filings are public records, and loan modifiers routinely swarm courthouses to find leads. Loan counselors at the Long Island Housing Partnership, a respected nonprofit in Hauppauge, N.Y., tell of scammers crashing its housing workshops, posing as troubled borrowers, then working the crowd with sales pitches.

And they do work hard. A call to one law firm's toll-free number plugged on WABC radio quickly gets a call back with a hard sell. "We have a 100 percent success rate" in renegotiating loans, an operator sweetly vows, reluctant to say more until you tell her what your mortgage payment is and how far behind you are.

The painful truth is that nobody has a 100 percent success rate, and not every loan is fixable. Banks have recently made public commitments to putting more effort into working loans out. But homeowners need to realize that the best way to do that is directly with the lender or through a reputable nonprofit counselor.

The for-profit loan modifier's cruelly deceptive sales pitch is that you get what you pay for. Nonprofit organizations, which work for no fee, say they can strike better deals, because they have longstanding relationships with lenders that storefront firms do not have.

But that doesn't mean that well-meaning advocates are aggressive and effective in finding people who need

help. The government, banks and nonprofit organizations need to be more creative and assertive to outmaneuver the predators — to send the competing message that hope doesn't require thousands of dollars in cash up front, although it does mean facing up to hard truths about one's finances and future.

Nonprofits frequently complain about how hard it is to get at-risk homeowners to ask for help. It's true that people deep in debt are often embarrassed and wrapped in blankets of denial. They don't open mail or reliably make appointments. But the good actors in this bad drama need to get better at working around that problem, before more good money is thrown after bad.

Copyright 2008 The New York Times Company

Privacy Policy | Search | Corrections | RSS | First Look | Help | Contact Us | Work for Us | Site Map

Alan Mehrwein

From: RMLS Communications [communications@rmls.ccsend.com] on behalf of RMLS Communications [communications@rmls.com]

Sent: Monday, December 01, 2008 3:30 AM

To: amehrwein@remax.net

Subject: RMLS Monday Morning Missives - December 1

12.1.2008 **RMLS™ Monday Morning Missives**

Trouble viewing this e-mail? Click here to view in your browser.

Private ID Change - December 10

Need help coming up with a new password?

Between now and December 10, you can voluntarily change your Private ID using the User Preferences option in RMLS*web*'s Toolkit.

On December 10, any RMLS™ subscribers who have not changed their Private ID in the last 30 days will need to do so before they are allowed into RMLS*web*.

Looking for ideas on how to create secure yet memorable passwords? Try this helpful guide from Microsoft.

As usual, if you have any questions or concerns we are here to help. You can call your local RMLS™ office or the RMLS™ Help Desk at (503) 872-8002 in the Portland Metro Area or toll-free at (877) 256-2169.

Listing Logic: Be Truthful in List Price

Listing at a lower price than seller will accept is unethical

Listing a property at a lower price than what your seller is willing to accept is a violation of RMLS™ Rules and Regulations (see section 8.5).

Properties listed for less than the seller will accept obviously attract attention because they are literally too good to be true. Enticing buyers with false information is unethical.

If you experience a situation where the seller or lessor of a listed property refuses to accept a written offer satisfying the terms and conditions stated in the listing, please report this to RMLS™ Rules and Regulations department at rules@rmls.com.

ActiveKEY Care

Use caution in extreme temperatures

It's getting cold out there, so keep in mind this friendly ActiveKEY battery tip from Supra:

"Temperature extremes can affect battery performance. If the ActiveKEY is below 0° C (32° F) or above 40 ° C (104° F), it will not charge. During very cold or hot times of the year, bring your ActiveKEY in from your car at night and between showings."

In This Issue

Private ID Change - December 10

Listing Logic: Be Truthful in List Price

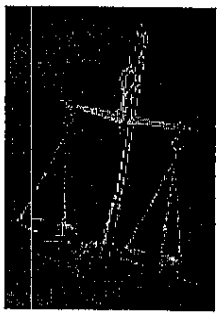
ActiveKEY Care

Test Your Rules Knowledge

What's New?

December Rules Change
Latest Market Action
Custom Columns Demo
Market Time Calculation (MP3)
eBilling Now Available

Test Your Rules Knowledge



Take the Rules and Regulations Quiz!
It's that time again. Test your RMLS™ Rules & Regulations knowledge by taking the latest quiz! Note: you will be prompted to run a Flash file.

Monday Morning Missives Archive

Looking for past issues?
Click here

Forward email

✉SafeUnsubscribe®

Email Marketing by

Strong passwords: How to create and use them

Published: March 22, 2006

Your passwords are the keys you use to access personal information that you've stored on your computer and in your online accounts.

If criminals or other malicious users steal this information, they can use your name to open new credit card accounts, apply for a mortgage, or pose as you in online transactions. In many cases you would not notice these attacks until it was too late.

Fortunately, it is not hard to create strong passwords and keep them well protected.

Related Links

- Check your password strength

What makes a strong password

To an attacker, a strong password should appear to be a random string of characters. The following criteria can help your passwords do so:

Make it lengthy. Each character that you add to your password increases the protection that it provides many times over. Your passwords should be 8 or more characters in length; 14 characters or longer is ideal.

Many systems also support use of the space bar in passwords, so you can create a phrase made of many words (a "pass phrase"). A pass phrase is often easier to remember than a simple password, as well as longer and harder to guess.

Combine letters, numbers, and symbols. The greater variety of characters that you have in your password, the harder it is to guess. Other important specifics include:

- **The fewer types of characters in your password, the longer it must be.** A 15-character password composed only of random letters and numbers is about 33,000 times stronger than an 8-character password composed of characters from the entire keyboard. If you cannot create a password that contains symbols, you need to make it considerably longer to get the same degree of protection. An ideal password combines both length and different types of symbols.
- **Use the entire keyboard,** not just the most common characters. Symbols typed by holding down the "Shift" key and typing a number are very common in passwords. Your password will be much stronger if you choose from all the symbols on the keyboard, including punctuation marks not on the upper row of the keyboard, and any symbols unique to your language.

Use words and phrases that are easy for you to remember, but difficult for others to guess. The easiest way to remember your passwords and pass phrases is to write them down. Contrary to popular belief, there is nothing wrong with writing passwords down, but they need to be adequately protected in order to remain secure and effective.

In general, passwords written on a piece of paper are more difficult to compromise across the Internet than a password manager, Web site, or other software-based storage tool, such as password managers.

Create a strong, memorable password in 6 steps

Use these steps to develop a strong password:

1. **Think of a sentence that you can remember.** This will be the basis of your strong password or pass phrase. Use a memorable sentence, such as "My son Aiden is three years old."
2. **Check if the computer or online system supports the pass phrase directly.** If you can use a pass phrase (with spaces between characters) on your computer or online system, do so.
3. **If the computer or online system does not support pass phrases, convert it to a password.** Take the first letter of each word of the sentence that you've created to create a new, nonsensical word. Using the example above, you'd get: "msaityo".
4. **Add complexity** by mixing uppercase and lowercase letters and numbers. It is valuable to use some letter swapping or misspellings as well. For instance, in the pass phrase above, consider misspelling Aiden's name, or substituting the word "three" for the number 3. There are many possible substitutions, and the longer the sentence, the more complex your password can be. Your pass phrase might become "My SoN Ayd3N is 3 yeeRs old." If the computer or online system will not support a pass phrase, use the same technique on the shorter password. This might yield a password like "MsAy3yo".
5. **Finally, substitute some special characters.** You can use symbols that look like letters, combine words (remove spaces) and other ways to make the password more complex. Using these tricks, we create a pass phrase of "MySoN 8N i$ 3 yeeR$ old" or a password (using the first letter of each word) "M$8ni3y0".
6. **Test your new password with Password Checker** Password Checker is a non-recording feature on this Web site that helps determine your password's strength as you type.

Password strategies to avoid

Some common methods used to create passwords are easy to guess by criminals. To avoid weak, easy-to-guess passwords:

- **Avoid sequences or repeated characters.** "12345678," "222222," "abcdefg," or adjacent letters on your keyboard do not help make secure passwords.
- **Avoid using only look-alike substitutions of numbers or symbols.** Criminals and other malicious users who know enough to try and crack your password will not be fooled by common look-alike replacements, such as to replace an 'i' with a '1' or an 'a' with '@' as in "M1cr0$0ft" or "P@ssw0rd". But these substitutions can be effective when combined with other measures, such as length, misspellings, or variations in case, to improve the strength of your password.
- **Avoid your login name.** Any part of your name, birthday, social security number, or similar information for your loved ones constitutes a bad password choice. This is one of the first things criminals will try.
- **Avoid dictionary words in any language.** Criminals use sophisticated tools that can rapidly guess passwords that are based on words in multiple dictionaries, including words spelled backwards, common misspellings, and substitutions. This includes all sorts of profanity and any word you would not say in front of your children.
- **Use more than one password everywhere.** If any one of the computers or online systems using this password is compromised, all of your other information protected by that password should be considered compromised as well. It is critical to use different passwords for different systems.
- **Avoid using online storage.** If malicious users find these passwords stored online or on a networked computer, they have access to all your information.

The "blank password" option

A blank password (no password at all) on your account is more secure than a weak password such as "1234". Criminals can easily guess a simplistic password, but on computers using Windows XP, an account without a password cannot be accessed remotely by means such as a network or the Internet. (This option is not available for Microsoft Windows 2000, Windows Me, or earlier versions) You can choose to use a blank password on your computer account if these criteria are met:

- You only have one computer or you have several computers but you do not need to access information on one computer from another one
- The computer is physically secure (you trust everyone who has physical access to the computer)

The use of a blank password is not always a good idea. For example, a laptop computer that you take with you is probably not physically secure, so on those you should have a strong password.

How to access and change your passwords

Online accounts

Web sites have a variety of policies that govern how you can access your account and change your password. Look for a link (such as "my account") somewhere on the site's home page that goes to a special area of the site that allows password and account management.

Computer passwords

The Help files for your computer operating system will usually provide information about how to create, modify, and access password-protected user accounts, as well as how to require password protection upon startup of your computer. You can also try to find this information online at the software manufacturer's Web site. For example, if you use Microsoft Windows XP, online help can show you how to manage passwords, change passwords, and more.

Keep your passwords secret

Treat your passwords and pass phrases with as much care as the information that they protect.

- **Don't reveal them to others.** Keep your passwords hidden from friends or family members (especially children) who could pass them on to other less trustworthy individuals. Passwords that you need to share with others, such as the password to your online banking account that you might share with your spouse, are the only exceptions.
- **Protect any recorded passwords.** Be careful where you store the passwords that you record or write down. Do not leave these records of your passwords anywhere that you would not leave the information that they protect.
- **Never provide your password over e-mail or based on an e-mail request.** Any e-mail that requests your password or requests that you to go to a Web site to verify your password is almost certainly a fraud. This includes requests from a trusted company or individual. E-mail can be intercepted in transit, and e-mail that requests information might not be from the sender it claims. Internet "phishing" scams use fraudulent e-mail messages to entice you into revealing your user names and passwords, steal your identity, and more. Learn more about phishing scams and how to deal with online fraud.
- **Change your passwords regularly.** This can help keep criminals and other malicious users unaware. The strength of your password will help keep it good for a longer time. A password that is shorter than 8 characters should be considered only good for a week or so, while a password that is 14 characters or longer (and follows the other rules outlined above) can be good for several years.
- **Do not type passwords on computers that you do not control.** Computers such as those in Internet cafés, computer labs, shared systems, kiosk systems, conferences, and airport lounges should be considered unsafe for any personal use other than anonymous Internet browsing. Do not use these computers to check online e-mail, chat rooms, bank balances, business mail, or any other account that requires a user name and password. Criminals can purchase keystroke logging devices for very little money and they take only a few moments to install. These devices let malicious users harvest all the information typed on a computer from across the Internet—your passwords and pass phrases are worth as much as the information that they protect.

What to do if your password is stolen

Be sure to monitor all the information you protect with your passwords, such as your monthly financial statements, credit reports, online shopping accounts, and so on. Strong, memorable passwords can help protect you against fraud and identity theft, but there are no guarantees. No matter how strong your password is, if someone breaks into the system that stores it, they will have your password. If you notice any suspicious activity that could indicate that someone has accessed your information, notify authorities as quickly as you can. Get more information on what to do if you think your identity has been stolen or you've been similarly defrauded.

↑ Top of page

Was This Information Useful?

Yes | No

© 2008 Microsoft Corporation. All rights reserved. Contact Us | Terms of Use | Trademarks | Privacy Statement