SHEAR BULL

Palm Beach County Roofing & Sheet Metal Contractors Association

UPCOMING EVENTS

DINNER MEETING

Self adhered application methods and most common application errors by Joe Thompson

Wednesday Sept 27, 6PM
Hilton Palm Beach Airport;
150 Australian Ave.
West Palm Beach, FL

ALL ABOUT PASSWORDS

Robert Ricketts, Palm Beach County I.T.; 561-818-1716; Robert@pbcit.com

Good news! The most commonly used password today is no longer the easy-to-guess "password". That's right! It's been replaced with "123456". We can all rest easy tonight!

Your password might not be either of those above, but there's a good chance it can be sussed-out nearly as fast. In this article, I'll discuss the state of password security today and what you need to do to stay safe.

Back in the day, an eight character password was considered reasonably safe. Not anymore. And just adding a couple of numbers to the end isn't going to cut it, either.

The following list of points are all recommended suggestions for maintaining high quality password security and integrity.

- Never use the same password on multiple web sites, especially those on which you've ever provided personal information, such as an online retailer, email, banking, brokerage, social media, etc.
- Passwords should be at least 15 mixed characters and the more the better
- Should not be stored in unprotected ways, such as the "Notes" section of your contacts. e.g. Storing your banking password in your contacts under the name of your bank is not good.
- Avoid logging into sensitive accounts from any computer that isn't under your full time control. Never use computers in a hotel's guest business center; there's a fair chance its been infected by a previous guest. Logging in using a friend's computer is safer but do so sparingly.
- Never connect your device to an open and unlocked public wi-fi. Passwords may be transmitted unencrypted which can be sniffed out of the air by any nearby bad actor. Use your own cellular connection only. If using a laptop, connect to the internet using your smartphone's personal hotspot feature.

Password Crackers are Smart

When a password cracker is trying to figure out passwords, s/he never starts with the "brute force" approach. Brute-force simply means trying every possible combination of characters. Yes, it's one approach they use, but it's slow compared to other approaches so they save it for last. Instead, they try popular password lists, common word lists, and apply programming rules in order to crack passwords without trying every possible combination. By combining these advanced techniques and using a very powerful custom-built computer, a password cracker can make billions of guesses per second! The rig pictured here costs less than $10,000, making it affordable to any determined hacker.

You might say "But how can a hacker make several billion guesses per second? No one can type that fast, and besides, won't the web site they're trying to break into limit the hacker to five or ten guesses?"

Yes, that's true enough, but that's not how password cracking works. Password cracking is performed offline against a stolen database containing thousands or even millions of usernames and passwords. Such offline attacks aren't affected by web server security that may limit you to five or so login attempts.

It's beyond the scope or the intended educational purpose of this article to go into the highly technical details of how, exactly, password crackers do their thing. Just please understand and accept that it's true.

So you'll want to create passwords that are hard for a password cracker to guess, even though s/he is making many billions of guesses a second. How to do that?

Continued on page 3....

2017 Officers & Board of Directors

Glenn Rimpela
President

Dennis Medaglia
Vice President

George Jacobazzi
Treasurer/Past President

Manny Oyola
Secretary

BOARD MEMBERS

- Ronney Taveras
- Mark Landis
- Ben Preston
- Mark Terlep
- Joe Byrne
- Jeff Eagle

Ronald A. Frano MBA
Executive Director

Legal Counsel
Trent Cotney, P.A. 813.579.3278

Program, Publication & Web
Joe Byrne 561-471-8363

Palm Beach County Board Representatives:

Construction Industry Licensing Board
Ben Preston, 561-964-7987

Construction Board of Adjustment & Appeals
Manny Oyola 561-436-5765

Building Code Advisory Board
Joe Byrne 561-471-8363

MESSAGE FROM THE PRESIDENT

Our August meeting was a bit anemic in attendance. August has never been a strong month for us and at one point we did not schedule a meeting in that month. We renewed scheduling them expecting to get a better showing but we realize that many of our members are not available during that day in August. Business trips, vacations and other conflicts seem to be common in the month. Our meeting in September should draw a sizable crowd. We have received interest from a couple of building department who want to have some of their inspectors attend. The presentation will be given by Joe Thompson, Member RCI who is the Commercial Roofing Systems Analyst for Certainteed. His topic will be Self adhered application methods and most common application errors. This should be of great interest to our contractor members. Please mark your calendar for September 27, 2017 and plan to attend. The board is also considering a BBQ picnic for the month of October. To date, we have not received a substantial interest from our members for such an event.

Hope to see you at our September dinner meeting.

Respectfully Submitted
Glenn Rimpela
President

Passphrases
Passphrases are an easy way to beef-up your passwords. It's better than using single-word passwords even with a number or two stuck to the end. If you met your spouse Sally in Memphis, how about something like "IMetSallyIn1990inMemphis". This password has twenty-four characters consisting of uppercase, lowercase, and numerals -- it's very strong and could likely never be brute-forced during the remaining time humans have on this planet -- certainly not within your children's lifetimes, anyway. Nor is it likely to fall to a rules-based attack where the cracker applies sophisticated guessing rules.

There's a webcomic called XKCD that's a favorite among geeks. One of his comics explains how a simple passphrase made up of four common words is more secure than pretty much any password most people usually think up

Popular Quotes as Passphrases
Do not use popular sayings or quotes. They are likely already cataloged in the word and phrase lists that password crackers use. e.g. The passphrase "FourScoreAndSevenYearsAgo" would be cracked in seconds even though it's nice and long.

Don't use bible verses. The entire text of the Old and New Testament is already cataloged. Probably the Torah and Qur'an, as well.

Don't use movie quotes. Pulp Fiction is choc-a-bloc with excellent lines and quotes which, in turn, makes them useless as passphrases. There's not a quote in the entire movie that would stand more than a few minutes in the hands of a password cracker.

If it's something you heard somewhere, especially if it's cool and memorable, then don't use it because the password crackers have literally heard and catalogued it all and they share with each other. The only passphrases worth using are ones that are personal to you that you make up yourself like the "Sally in Memphis" example. Although now that I've included the Sally in Memphis passphrase as an example in this article about passwords, it probably won't be long before it's no good, either. And, of course, any version of "correct horse battery staple" is totally off-limits.

The key is to choose a passphrase that exceeds twenty characters. For extra strength, include at least one uppercase, lowercase, and a numeral. You can include a special character, too, but given the length (20+), that's not really necessary.

Password Management -- Remembering all those bloody passwords
Even though passphrases can be easier to remember than a deliberately mangled single-word password, you'll still need to remember a lot of them if you want follow good password hygiene. There's several of approaches you can take here.
The best old school approach is to buy a spiral notebook and dedicate one page, front and back, to each web site. That way, you have plenty of room for notes and corrections associated with each web site. Use a pencil so you can edit later. Jot down everything you'd ever need to know: Username, password, answers to security questions, account numbers, etc. A spiral notebook cannot be hacked so it's actually a very safe way to record passwords. Write neatly in block letters and not your sloppy cursive so you can read it later.

Another approach is to save all your passwords in a password-protected Word file (Use a passphrase here, too). Then every time you edit and save the file, print it out as well so you'll have a hard copy, in case your computer dies.
And yet another approach is to use a password manager program. These are database programs that store passwords, synchronize them between various devices, and auto-fill password boxes in your web browser. But such approaches do require some dedication to the task, so to speak.

Continued on page 5....

SATURDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
					1	2
3	4	5	6	7	8	9
	Labor Day					
10	11	12	13	14	15	16
	Patriot Day					
17	18	19	20	21	22	23
				Rosh Hashanah	First Day of Fall	
24	25	26	27	28	29	30
			Dinner Meeting			

PBCR & SMCA Office and Phones:
2101 Vista Parkway, Suite 4001,
West Palm Beach, FL 33411
pbcroofers.com
facebook.com/groups/269143749847473
Tel: 561.655.5393 | Fax: 561.688.8807
Ronald A. Frano, MBA, Executive Director
rfrano@pbcroofers.com

More on Password Managers

Password Managers are programs that, well, manage passwords. But they do it safely and offer additional features. The hold all your passwords in a secure database that is, itself, protected by a master password. PMs can also auto-fill password boxes in your browsers and help you generate super-strong passwords for new online accounts that you create.

All the popular browsers (Chrome, Firefox, Safari, etc.) also have password remembering features, though that's usually all they can do. They do not generate fresh passwords nor can they work on multiple browsers. e.g. Chrome, Firefox, Safari, Internet Explorer, Edge, Opera, etc. each save your passwords in it's own database, so you'd have to separately teach each browser you use. A proper password manager like LastPass or 1Password can auto-fill your passwords into any browser once it's learned your passwords.

Password managers also help protect your from phishing emails that try to trick you into logging into fraudulent, look-alike, web sites. While you as a human may be fooled by a fake Bank of America login page, a password manager would never be tricked in such as way. Using a password manager, you'll know right away if a login page is fake because the password manager will refuse to auto-fill the username and password.

Another advantage to password managers is they free you from having to remember passwords at all. And since you no longer need to remember them, the PM is free to create very long and totally random passwords that are insanely secure and could never be cracked. That's the best password of all: Very long and totally random. e.g. "[f}<LCn)+-C#nhc/Y7us`m3v~D9N/3" is long, random, and ultra-secure.

Passwords managers automatically sync between your devices so you should rarely have to manually type a password again.

Two Factor Authentication

Two Factor Authentication, or 2FA, is a feature offered by more and more web sites these days. When a web site account is protected with 2FA, then you must provide two different forms of identity in order to access the account. The first is your password as usual, and the second is generally a random six digit number displayed on your smartphone. This way, if a hacker managed to figure out your password, s/he would be unable to access your account because s/he would not have your smartphone and, ergo, the six digit number.

The web site TwoFactorAuth.org lists hundreds of popular web sites and whether or not they offer 2FA. Check to see if the web sites that are important to you offer 2FA. If they do, then take advantage of it! If not, complain to the website owner.

Setting up 2FA is not entirely painless. It must be done correctly lest you lose access to your own accounts. e.g. Authorizing your phone to be the security token, creating emergency backup code keys, setting up alternate email address for account recovery, etc. This is where a guy like me comes in. I know how to set these up properly to keep you safe!

Brave New World

Security professionals everywhere constantly grapple with these opposing forces: Security vs. Convenience . TSA, metal detectors in federal buildings, pre-employment background checks, random drug testing, and now immigrant background checking. Same thing applies to computers and web sites. Greater security means more hassles for legitimate users.

Imagine the ruin you could face if your bank or brokerage accounts are hacked into. If your business email or cloud accounts like Dropbox were hacked and your confidential info or your client's was ransacked and exposed, your liability would be limitless.

I know that all the things I've discussed and suggested above can be unnerving and even a pain in the ass to follow. Who can remember hundreds of passwords that all have to be different and complex? But this is the reality of living online today. Security is simply too important to neglect and as our lives and businesses are ever more conducted online, good security is absolutely critical. Disregard at your peril.