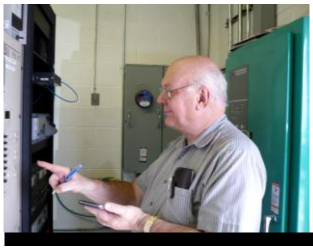

The

Broadcasters' Desktop Resource

www.theBDR.net ... edited by Barry Mishkind – the Eclectic Engineer

Bits and Bytes

Do Not Neglect Password Security

[November 2011] Have you changed your passwords recently? Read on. You might just decide it is a good time to do more than just think about it.

A generation or so ago, most people did not lock their homes or cars. Keys were left in open sight – in the ignition, for example – in case a neighbor came calling and needed something.

By and large, those days are gone for most of us.

Today, securing valuables is much more complicated. Not only do we have locks and keys, but sometimes the most valuable things are protected by our user passwords.

BIG TROUBLE

Here is the problem: if some bad actor manages to get even one of your passwords, it truly can create some tremendous problems.

In short order, you could find your bank accounts drained, your personal information used for identity theft, and your email address book can be used to spam your friends and business acquaintances or, worse, to push viruses and/or Trojans on them.

If it has not happened to you, it *has* happened to thousands of others. It is, unfortunately, a real, living nightmare. Victims wake up and check email to find one of these several situations:

1. There is no email. Somehow it was all deleted.

2. Their inbox is filled with dozens (hundreds) of bounces and outraged complaints due to spam and other bad emails that originated from their account.

3. They cannot access your email at all. The password does not work. They are locked out!

And that might only be the start if your email password has been taken.

MULTIPLE ADDRESSES

Suppose someone now has your email address and password. Some will say, "Oh, if I lose an account at Yahoo or Hotmail, I'll just open another." But that could lay you open to some real nastiness.

Here is what can happen if someone gets control of any email account, even one that is the "alternate contact address:"

A hacker managed to get inside the mail servers at a major email host, and they grabbed some accounts and passwords. They then tried all the various financial sites and – surprise! – one of the email addresses worked.

Using the "forgot my password" feature, the hacker got the bank account to send the password in seconds and, you guessed it, all the money disappeared. And now that the hacker had a second password, he could try that and see if it worked on other sites. This could be an expensive game of dominos.

If you ever wonder whether your email account might have been hijacked, one on-line listing to check is at https://pwnedlist.com/ While not 100% certain, it does have a database of over five million email addresses that have been compromised.

In any event, it is a worthwhile effort to list all your various email addresses and ensure no account or password is "hanging out" unprotected. It may not be an easy task, especially for those who have been on the Internet for a long time. But it seems worth the effort to make sure none of those old addresses can cause you trouble.

SECURE PASSWORDS

As you can see, whether you are using one email address or a dozen, the associated passwords need to be secure,

Far too many people use one password for all their various accounts. The most used password? A study of 32 million passwords stolen last year found that "123456" was the most common password – over three times as common as #2: "12345"

Also in the Top Ten: password, iloveyou, and abc123. Studies also show over half the passwords used are seven characters or less, and 36% used words found in a dictionary of commonly used passwords.

The reason for this is that too many people simply have a hard time remembering all those long and involved passwords the IT department often kicks out. (Have you ever seen a password written on a post-it note stuck on a monitor? Enough said.)

So, now what?

PASSWORD CALISTHENICS

Some sites have forced users to exercise a bit and pick longer, stronger passwords. Other sites will attempt to analyze your password and give advice on whether it is good or not.

For example, Steve Gibson has an interesting password evaluation page, with a discussion on the issue. You can find it one the web at: https://www.grc.com/haystack.htm

What is really scary is to see estimates of how fast a password can be broken by brute-force techniques. What is helpful is to see how easy it is to strengthen your password to the point that most hackers will go away. (As with most criminals, if you make them work at it, they generally will go elsewhere.)

Of course, in response, hackers have developed more programs designed to crack passwords. Some are brute force attacks, literally using the dictionary, as well as a list of the most used words and common variations, such as PASSWORD, PaSsWoRd, PASSword, etc. If your account is attacked, you can be sure these will be tried.

Since most people use all lower case characters in their passwords, a quick way to provide some strength is to use a capital letter, a number, or a special character – or all three.

Usually the best passwords mix upper and lower case letters with numbers and at least one special character. A phrase that is slightly turned so it is not all dictionary words is a good start. You can remember a phrase, insert some "….." or perhaps "@*&!" in the field, and now you have a non-dictionary password that is hard to crack.

Oh – just in case you were thinking to use a zero for an o, or the number one for an l, remember, the hackers know those tricks – they use them themselves – and will try them. So something like passw0rd is most certainly not safe!

GUESSING AND ENGINEERING

Other hacker tactics that cause people to have their computer accounts are so simple as to be alarming.

The Florida hacker who guessed passwords of some famous people is an example. If you talk about your cute puppy or something that means a lot to you, most hackers see a password ready to be given up. Indeed, many people use passwords that describe themselves, their families, or their pets. As in many TV shows or in the movies, hackers often start with what they know: birthdates, children's names, pet's names, etc.

Of course, you can never protect yourself enough if the computer host or IT support personnel can be scammed by phone. The story of a wife afraid her husband is going to drain their bank account has caused more than a few support people to cough up (or reset) a password.

EXTERNAL AIDS

Icons are sometimes presented in an effort to protect users from thinking a fake site was real, and entering their password for scammers. But the best protection continues to be a strong password.

Here is another site that will show you graphically how to create a stronger password, one that will generally keep you safe: http://www.passwordmeter.com/

And there are numerous programs and even hardware that lets you carry your passwords along with you, like your house keys. Plug them in and they will handle involved passwords without you having to stop and think about it.

BEST EMAIL PRACTICES

As you work to protect your email and other accounts, here are some of the key things to remember:

1. Use a unique password for each computer account you have, including each email account.
2. Use a long, strong password that is not easily guessed or compromised by a dictionary attack.
3. Change the passwords regularly – maybe once every three or six months
4. Do not write the passwords down anywhere.

Being realistic, though, almost no one actually does this. So, if you cannot handle the above, try doing at least this much:

1. At least use different passwords for anything sensitive. (casual log-in websites aside)
2. Build a password with multiple words and characters.
3. Use a solution like a password generator.
4. Use a flash drive or password saving program.

To make it harder for the bad guys stay away from 123456 (or 654321). Again, as with doors and fences, crooks do generally take the easiest route. So if you use the ideas presented here, it will cause most attackers to pass on and go after an easier to crack password.

Generally, if you build your own passwords, rather than use a generator, you will be able to construct some relatively easy to remember passwords that score high on the security estimators.

By using the suggestions here, you should have one less thing to worry about these days. And that is something good.

Return to The BDR Menu