The

Broadcasters' Desktop Resource

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

Bits and Bytes

Discovering If Your Credentials Have Been Pwned

By Barry Mishkind, BDR Editor and Publisher

[July 2020] Computer security covers a lot of areas. We need to protect ourselves, personally, from hackers and websites trying to push malware and ransomware on us.

Have you ever noticed a sudden surge in spam coming to your email inbox? Or, how about an email from someone claiming to know your password – even showing the password – and threatening to post nasty videos of you on the Internet unless you pay them?

Unfortunately, each year the Internet gets more like the old "Wild West," and no safer. Daily amounts of spam emails can easily outnumber wanted email … or worse.

All it takes is just one careless click and your entire LAN can be brought down, as evidenced by the experiences of many large companies – several of them in the broadcast field. As a result, a lot of companies have begun to avoid putting email addresses on their websites, to prevent "harvesting" and/or "spearphishing" by crooks.

For these companies, sometimes the only way to contact them is via a web form.

WHAT IS GOING ON?

Ever since the early days of Internet email, there have been hackers and groups that "scrape" every possible website and email conversation group to grab email addresses. Now, they break in to steal credentials from servers.

How successful have they been? According to some experts, something over 9,765,110,880 user accounts and 572,611,621 passwords have been exposed in data breaches. These are sold and resold for pennies per address – and form the basis for billions of spam messages a day. (Current statistics say nearly half of the 29 billion emails sent around the globe each day are spam.)

Each user is then forced to use filters, blockers, and exercise special care not to click on the wrong thing.

And still they can be compromised.

A TEAM EFFORT

Clearly, cyber security is a team effort. As much care as you put into doing things securely, one careless person can quickly crash everything around you – and that is scary, especially in a broadcast environment where many people must have access to mission critical systems.

While the so-called Nigerian Scams – including strange English wording and offers to share astronomical amounts of money – are still effecttive, stealing large sums every year, some of the tactics used by criminals have become quite sophisticated.

For example, using one valid email address, hackers will try to send email to everyone in a company, hoping one will click on a link installing malware. Or, once they know the manager's and bookkeeper's email addresses, some will try to spoof a message instructing the bookkeeper to send money to a new account.

UNDER ATTACK

Worse, once the bad guys know your user account name, they will try every possible website, including banks, to seek ways to steal your assets.

But, you say, how could they know my password?

Easier than you might think.

First, far too many people use "password" or "123456" – or some minor variation – and use that on multiple sites. When they find a working account, they will try every possible password, depending upon how a server is set up, they could try hundreds or thousands in a short time.

And after one site is broken into, the bad guys will try any site they think you might be connected to, from banks to streaming video sites. It is all automated and if you ever look at server logs, you will be stunned at how many attacks go on each day, even to "obscure" web sites.

STRONG PASSWORDS ARE NO SAFER

But suppose you have a strong password. Lots of letters and numbers and symbols.

Again, someone else – someone with no relationship to you other than being a user of a web site you have signed onto – can cause your credentials to be compromised.

Here is how: Let us say that john@doe.com has an account at the Acme Parts Company, a place you shop. John has used "password" as his password. Dumb, right? No, dangerous. A hacker who breaks into the Acme Parts server can take records of thousands of accounts and passwords in an instant.

And, here is the really frightening part: even though the passwords are encrypted, as soon as they locate John's account, you are potentially compromised, too!

What happens is that John's password may be encrypted to something like "K8*tg34S." But the hacker knows it is really "password." So the bad guys simply run a series of various decryption programs until they turn K8*tg34S back into password. Now they can do the same to you, decrypting your password with the same algorithm. Once again, then they try any place you might have an account, trying to break in.

WHAT PROTECTION IS AVAILABLE

The first step every security person advises is "use a different password – and never "password" itself – on every site you visit. Additionally, whenever possible use a different account user name.

That reduces the chances a break-in at Acme Parts will affect your account on another site.

There are several good applications that will keep track of your accounts and passwords, themselves protected by a master password.

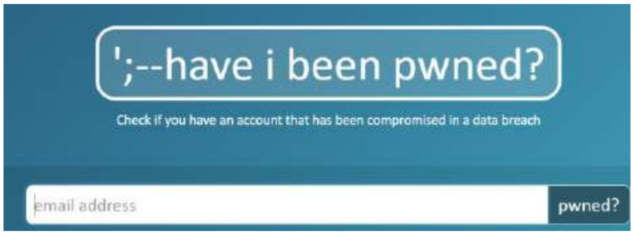
Seems reasonable.

Nevertheless, the alarming number of data breaches still provides the bad guys with lots and lots of potential targets. The current "fix" is to use something called 2FA – Two-Factor Authentication – where available. The idea is that if you enter your basic credentials, the site texts a code to your cell phone, so even if someone actually knows your password, they are blocked – unless they have your phone.

IDENTIFYING PWNED CREDENTIALS

Perhaps you want to know if any of your credentials have been compromised.

There are several places on the Internet to uncover pwned credentials. (Pwned is hacker-speak for "Owned" with "O" being right next to "P" on the keyboard). For example, there is a website, haveibeenpwned.com, that makes available to you a quick check as to whether any of your accounts or passwords have been compromised.



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

One of the newest options is the Password Checker feature on the Chrome browser. (Go to Settings/Safety Check.) It alerts you if a password entered is compromised. For more detail, log into myaccount.google.com/security-checkup, which will lead you to Password Checkup. There, you can learn if you have compromised passwords, passwords used on multiple sites, or passwords deemed insecure. You might surprise yourself.

In conclusion, we hope that you and all your co-employees practice the safest of computing, but do stay vigilant. If you learn you some of your credentials are compromised, take the clear warning so that you can change them before any of the bad guys comes looking. **-BDR**

- - -

Are articles like this useful to you? Then you are invited to subscribe to our one-time-a-week Newsletter, which is designed to let you know what is new. [Just take 30 seconds and click here.]()

- - -

Return to The BDR Menu