THE SIMPLE GUIDE TO HACKER-PROOF PASSWORDS

Learn How To Create Hard-To-Guess Passwords And Protect Your Organization

Provided by:
Leia Shilobod, CEO
InTech Solutions, Inc.
www.intechit.net
724.235.8750

InTech SOLUTIONS

From The Desk of:
Leia Shilobod | CEO, InTech Solutions, Inc.

Dear Colleague,

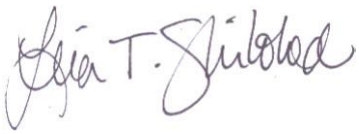
If you are the decision maker in a business, this report contains important information that will be extremely valuable to you to safeguard your firm through the most overlooked thing that can GREATLY increase security: PASSWORDS**.**

My name is Leia Shilobod, CEO of InTech Solutions and author of "Cyber Warfare: Protecting Your Business From Total Annihilation." We've been providing IT Consulting and Cyber Security Services to businesses for over 13 years now.

Passwords are the bane of our existence: you have to remember so many and change them all the time. How do you keep it all straight? That's why I created this easy guide to help you.

In the end, my purpose is empower you and help you make the most informed decision possible about the security of your firm so what you worked so hard to build is protected.

Dedicated to serving you,



"The Password Problem"

If I had a dollar for every time I broach the subject of secure passwords with business owners and executives and they roll their eyes I could close my IT business and retire quite comfortably.

Why am I getting that response? Because THEY KNOW. Everyone knows the need for better passwords and password management, but still I get eye rolls.

Let's break it down a little.

Imagine your business is like a house. The house has many doors and windows. If you were smart and wanted to protect your house from criminals, you put locks on all the doors and windows. When you set a password, it is like locking your doors and windows on your house.

A password is like a key. There are all different types of keys: big ones, little ones, strangely shaped ones. If someone found a key, it would only be useful if they knew what lock that key opened. Let's say someone was walking around outside your house and found a key, they would most likely assume it opened one of the locks to your house. There is a high probability it does.

If someone found a key in a public place, say, at the grocery store, if it had a label on it "427 Anderson Street Front Door Key" they could match that key to a lock on your house. If there was no identifying label, they would probably have no idea what lock it opens.

Now, if they are a cunning crook, they know keys are useful even if you don't know what it goes to, so they keep the found key. And as they continue to find keys, they keep collecting them.

Then, when they want to rob your house, they take their stash of keys with them and try them all in all the locks to your house. It turns out one of them works, because it's actually used in some other houses too.

"What Does All This Mean?"

If the house is your business, the doors and windows are all the ways you can access your company such as a computer connected to the internet, your firewall, or someone walking into your business and plugging in a jump drive.

Finding a key outside your house and assuming it goes to one of the locks there is like leaving passwords on your monitor, under your keyboard, taped under the firewall, written in a document saved on your network, or book/planner you take with you.

It's safe to assume that password is to something on your network, so they only have to try all the locks to get in.

Now to explain the key found in the grocery store, or the stash of keys the crook used to break into your house. Cyber criminals don't have to manually try all the passwords that they have a 'stash' of at one of the 'locks' to your 'house.' Cyber criminals have software that uses complicated algorithms to determine just which 'key' goes to your 'house.'

But YOU have the power to make this key finding process a walk in the park for cyber criminals, or you can make it dang near impossible for them to crack it.

"So, What Passwords Are Definitely Not Secure?"

Right here, right now, vow to change your password habits.

If you promise, I will divulge to you the secrets of creating and maintaining secure passwords.

Ok, I'm going to tell you anyway, but for the love of your bank account and your business, please do change your habits immediately.

Let's start by identifying what a BAD password is. The following list is the top 34 passwords used in 2017.

- 123456
- Password
- 12345678
- qwerty
- 12345
- 123456789
- letmein
- 1234567
- football
- iloveyou
- admin
- welcome
- monkey
- login
- abc123
- starwars
- 123123
- passw0rd
- master
- hello
- freedom
- whatever
- qazwsx
- trustno1
- 654321
- jordan23
- harley
- password1
- 1234
- robert
- matthew
- jordan
- asshole
- daniel

This list changes each year, but MANY remain on the list year after year. Repeat offenders include: 123456, Password, 12345678, qwerty, 12345, 123456789, football, welcome, abc123, dragon, passw0rd, and master.

We also find that many people choose passwords associated with pop culture. For instance, during the election we saw many election related passwords such as 'trump,' 'Hillary,' 'prez2016,' etc. Last year we saw 'starwars' hit the top passwords the list due to the box office hit. I cannot stress enough to steer clear of pop culture terminology in your passwords. They are written into hacker algorithms and easily cracked.

"How do you know those are the top passwords?" you may wonder…

Data is aggregated from many sources, but especially from credential breaches posted for free or for sale on the Dark Web. It doesn't take much crunching to see which passwords appear most often.

So now that you know what passwords to NOT use, how do you determine what password to actually use?

"The Pain of Password Changes"

For years IT Security Professionals preached the necessity of changing passwords at least quarterly. The idea was that if a password was compromised, it would only be useful for no more than 90 days. In many cases that's not long enough for a criminal to determine where the password goes and gain access to that user's resource the credential unlocks.

It turns out this practice actually makes it EASIER for hackers to crack your password. Let me explain. Let's say your password is JUNApr1c0t$2018. You use Apr1c0t$ (apricots) as your base password because you love apricots, then JUN because you last changed your password in June, and 2018 as that is the current year.

When password reset time comes in September, you change your password to SEPApr1c0t$2018. Why? Because you had to change your password in 5 other places and this is the method you employ in desperation to try to keep your passwords and multiple changes straight.

I'm actually being gracious thinking that you all are using at least 15 characters, complexity, and pre-pending as well as appending dates. Most people just use Password1 then change it to Password2, Password3, etc.

I have seen this in the wild, people, so I know it's true. If this is you, STOP IT NOW.

Why? Because hackers KNOW you do this. They are not dumb people. They build this kind of known user behavior into their algorithms, too. If you continue this practice, you are kidding yourself and leaving yourself wide open for hackers to crack your password.

For this reason, in 2017 NIST released Special Publication 800-63B which details that users should no longer be forced to arbitrarily change their passwords, but rather passwords should only be changed if users 1) forget or 2) are compromised.

"Proper Password Standards For Our Day & Age"

Your password should have at least 15 characters, but security professionals recommend 25. It turns out that LENGTH is the key to making a secret password more secure.

Even though length is key, be sure to give your password complexity by having a mix of numbers, special characters, capital, and lower-case letters.

Your password must also be secret. That means you should not tell it to anyone, nor should you write it down in a place that someone could find it.

Access to a password means that anyone can essentially be you. It is the most basic way of stealing your identity.

If I have your Windows password for your network and I log in as you and delete a bunch of files, YOU have deleted a bunch of files. If I log into Facebook as you and post racial slurs, YOU have posted racial slurs.

This is why it is absolutely essential your password remains secret.

You must also have a variety of passwords. This means using different passwords for different websites and still different passwords for accessing your computers.

Another strategy hackers use to leverage themselves into your accounts is by getting just ONE password and access to just ONE account.

Then they try to access the most common sites used by the majority of people such as Facebook, LinkedIn, Microsoft Office 365, gmail, Dropbox, and PayPal, and major banks. To use the illustration above, one key to your house can open many locks.

For this reason, each website you access should have unique and distinctly different passwords.

"I've got it," you say, "I'll just have my browser remember my credentials so I don't have to!" Nice try, but no dice. Although it is easy to do, and often times your internet browser prompts you to save your credentials – DO NOT DO IT.

When your computer or mobile devices gets infected by malware, these stored passwords are culled and cracked. And as we've already learned – you've just gotten hacked or you're going to be hacked again really soon.

"Why Your Password Strategy Sucks"

Now that I've officially shot down your favorite passwords and told you that you now have to remember 1,000 different passwords that are 25 characters each, however is a person supposed to create a password can be remembered and how on earth does one keep track of them all?

Let's first talk about password creation strategy.

To attain a password that is 25 characters in length, think of it as more of a **passphrase** instead of a password. That will start to get your head thinking in the right direction.

First, you must stop picking bad passwords. Here's a peek at how you're picking really bad passwords when you think you're being clever:

- Your "random" string of words will be something like "footballpatriots4thewin," which are **extremely common words**, and a hacker's algorithm will crack it.
- You'll pick something memorable, which will limit your options; **it will be something too simple** and a hacker will crack it.
- You'll manage to make a password this **super secure, then you'll forget it** and revert back to a weak password, and a hacker will crack it.
- You'll pick something **identifiable to anyone** who follows you on Twitter or Facebook—like your dog's name—and a human will guess it.

I have mentioned several times about hackers cracking passwords and now is a good time to go a bit further into what I'm talking about, so you understand what you're up against.

The programs hackers use to crack passwords ("crackers") are sophisticated. They know that most passwords consist of some sort of root word with something appended onto the end.

These crackers use many different dictionaries for root words such as: English words, foreign words, proper names, and phonetic patterns. Then they use two digits, dates, single symbols and so on for appendages. They also run the dictionaries with various capitalizations and common substitutions such as "$" for "s", "@" for "a", "1" for "l" and so on. This guessing strategy quickly breaks about two-thirds of all passwords.

Using this strategy, could a cracker crack YOUR password?

"How To Create A Secure Password"

As mentioned earlier, consider a phrase that would be memorable to you. Let's say "Merrily we roll along." That's pretty easy to remember.

If you used the old strategy, this would become something like "M3rrilyW3R0ll@long." And it would be easily cracked. Instead, try modifying the phrase so the words aren't easily identifiable by a cracker, like: "M@rly(we)r~llal000ng" or "!Murly-weeer0lalng"

Do you see the difference?

Need more ideas?

Think of a favorite line from a movie, your favorite poem, or a song. Choose the first letter from each word and include capital letters, numbers and a special character.

For instance, "Toto, I've got a feeling we're not in Kansas anymore." becomes: "T0t0!gafwniKa*"

Our brains are actually pretty good at subbing the strange characters and capitals when we remember the phrase in our heads.

Try just one password and see how it goes… you'll surprise yourself!

"So I Got A Strong Password – But How Do I Store It?"

Now let's discuss how to store passwords. If you write the password down on a post-it note and stick it to your monitor it ceases to be secret, and therefore, no longer secure. The most complex and long password imaginable that is written down and easily found totally negates your efforts.

There are a few schools of thought on how to store passwords and there is controversy and nay-sayers for each method.

Let's look at them.

The first method is to remember all your passwords and passphrases by route memory. This method allows all passwords to be locked inside the super computer that is your brain, only to be given away by you.

The great thing about only having memorized passwords is that they start, stop, and end with you alone. There is no one or nothing (except a compromised computer!) that can get their hands on your password.

Unfortunately, our elegant brains are not very good at calling up information when we need it. Your passwords can get lost in there. What we call forgetting. Additionally, if something were to happen to you, rendering your unable to recall most things, those passwords would be lost forever.

For this reason, many security experts do not recommend only storing your passwords in your memory. (That and many IT professionals get all pissy when they have to constantly reset user passwords.)

The next method is to **employ a password manager software.** This software lives on one or more devices (your laptop, your mobile phone, your laptop, etc.) and stores all your passwords in an encrypted format. You only have to remember ONE master password to access all the other passwords.

There are several things to consider when employing a password manager software.

First, there are hosted solutions such as LastPass and 1Password. These companies save your passwords on their servers in an encrypted format so that you can easily sync the manager across your devices.

A hosted solution takes the management of the software away from you. If the hard drive on your device fails, and that is the only location your passwords are stored, you just lost them all. If the passwords are hosted elsewhere, you still have them in the company's "cloud" location.

The hosted services do allow you to store an offline copy in a protected folder, but the management and protection of that file is on you.

There are also passwords managers that live locally on your computer only. For the more paranoid of us, and those willing to put in the extra work of having a local manager, this solution may be a good fit.

Solutions like PasswordSafe are free and open source. They are easy to set up even if you aren't too tech savvy, as long as you follow the instructions.

Because the software is stand alone and could be hard to manage between devices, it allows you to keep the password database on a USB jump drive and plug that into the machine you are using, launch the software, enter your master password, and have access to all your passwords.

Regardless of the solution you choose, carefully read the FAQ, installation, and use instructions to assure you will be happy with the product. Also verify pricing so you aren't surprised later.

Most password managers have a random password generator function to have the computer quickly create strong and complex passwords for you. Since you are storing the passwords in the manager software they don't have to be memorable.

If you employ a password manager software, I highly recommend you take advantage of this feature. Assure there are at least 12 characters in the passwords generated for you.

The final method is tried and true, and may actually surprise you: writing the passwords/passphrases down and storing them in a locked drawer or cabinet.

That sounds awfully elementary and low-tech. Indeed, it is. However, this is still an approved method of storing passwords at the highest and most secure levels of our military.

Why? Is the military just living in an archaic bubble that hasn't come up to the sleek standards of today? No, and in fact, this method assures continuity of the passwords.

If something should happen to you, someone can be alerted at the time of an incident and gain access to your written passwords. Since so many of our lives are tied to digital accounts, this is very important.

Let's say your mother becomes incapacitated and is in a nursing home, unconscious. You need to be able to pay her bills and access her insurance information. But you don't have access to any of her accounts. And guess what? The bank and insurance company won't talk to you. If you don't have a power of attorney set up already, you'll need to contact an attorney, invest a lot of time and money, provide that to the bank and insurance company, then they will start to talk to you.

If you are able to access her accounts immediately, there is less pressure to get the Power of Attorney. You'll still need to get it so you can make decisions on her behalf, but it's one less stressor while you're in a bad place.

Passwords ARE a big deal, so choose yours wisely and store them properly.

If you need help selecting and implementing a password manager or if you'd like to have Leia deliver some Cyber Security Training for your team, contact Leia at Leia@intechit.net or call 724.235.8750.