Password Security

The Story of John's Password

Lets begin this section by considering John Smith, an entirely fictitious employee at Acme LTD. John has recently received a prompt to change the password on his computer. John has a tendency to forget passwords, so decides to base his password on something familiar to him: his name. John vaguely remembers reading something in the company security policy a few years back about strong passwords, so he decides to substitute the 'o' in his name for a 'O', the 'S' for a '$', and the 'i' for a '1'. He throws in a few exclamation marks for good measure, so his new password reads **JOhn$m1th!!**

"They'll never guess this one" , thinks John to himself.

How long do you think it would take a half-decent hacker to crack John' s password?

We'll tell you at the end of this section!

Hackers Love Weak Passwords

It would probably surprise you to learn that the most hacked password in the last few years is **123456.** According to the UK's National Cyber Security Centre, some **23 million** accounts 'protected' with this password were hacked last year. Here' s the full top 10:

1. **123456**
2. **123456789**
3. **qwerty**
4. **password**
5. **111111**
6. **12345678**
7. **abc123**
8. **1234567**
9. **password1**
10. **12345**

Is Your Password Secure?

The passwords listed above are very obviously weak, but people still use them. You might think to yourself, 'I would never use a password like THAT', but your own password may be more easily cracked than you think!

Hackers are **very good** at what they do. They use software that can test thousands of passwords per second. For example, running a hacking program that inputs a list all words in the English language will crack **30%** of all passwords in less than **1** second. Hacking programs can also rapidly test passwords containing common substitutions, for example, those using capitalization (october = October), or letter/number swaps (october =Oct0b3r), or other password variations.

Don't Make it Easy!

Often, people can make life easier for hackers by unwittingly providing clues as to what their password might be. For example, if you proudly proclaim to the world that you are a Liverpool FC fan on your Facebook page, hackers (or any less-than-scrupulous person)may deduce that there is a fair chance that your password is based on something Liverpool FC-related. This goes for anything you post in the public domain: your favorite film, music, pet, or the names of your children.

Never base your password on information you post on social networking sites, or other public domain!

Change the Default

Another way in which you can make like easier for hackers is to not change the default password on your computer, smart phone, firewalls or other application. Default passwords are those pre-configured passwords or codes that come with new devices. They are intended to be used for initial configuration only, but very often they are not. **Hackers know and exploit this.**

Common default passwords include **Admin**, **Password**, **12345** among many others. In fact, there are hundreds of websites that list the default passwords for practically every device you can think of.

Always change the default password on any device before you use it!

Bad Passwords

Which of the following passwords is likely to be successfully hacked? Answers are on the next page!

A) Password

B) Pa$$w0rd

C) Ar$3na171

D) 895387

Answers

The correct answer is that all these passwords are open to hacking!

Password: This one should be obvious!

Pa$$w0rd: Would be instantly cracked as it is well known and uses common substitute characters. -

Ar$3na171: Somewhat stronger, but based on the word 'Arsenal' and using common substitute characters ($, 1). Even more hackable if it is known that the holder is a fan of Arsenal FC.

895387: Never use a password consisting of numbers only - they are extremely easy to crack, regardless of length.

Creating a Strong Password

Now that you now know how **not** to create a strong password, let's look at how you create a strong one.

Tip 1

Think of a Sentence

Think of a sentence or phrase that is familiar to you but not to others. For example: “My dog's name is Rex”

Tip 2

Convert It

Convert the phrase into a password. Use the first letter of each word to form an acronym, e.g., mdnir

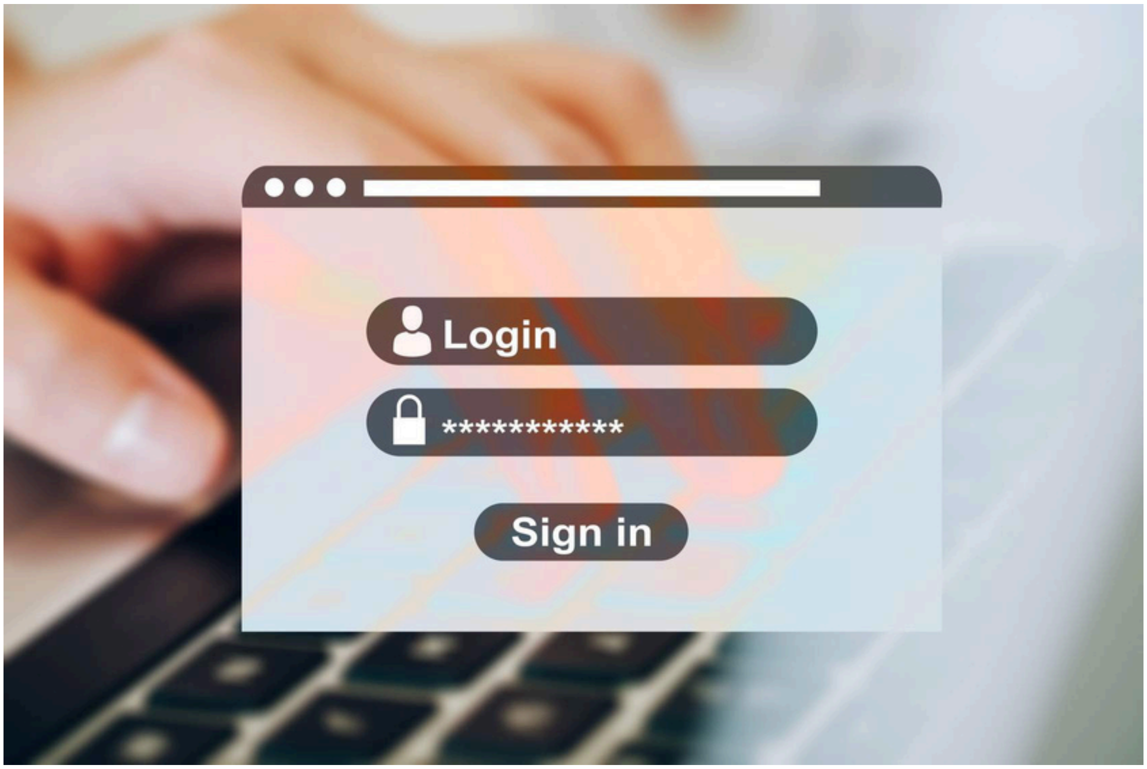
Tip 3

Add Complexity

Add complexity. For example, you could add extra characters between the letters to give m$d$nir* or you could make more complex by mixing upper and lowercase letters e.g. M$D$nir*. Alternatively you could use “rx” for Rex to give m$d$nirx which might be a little easier to remember.

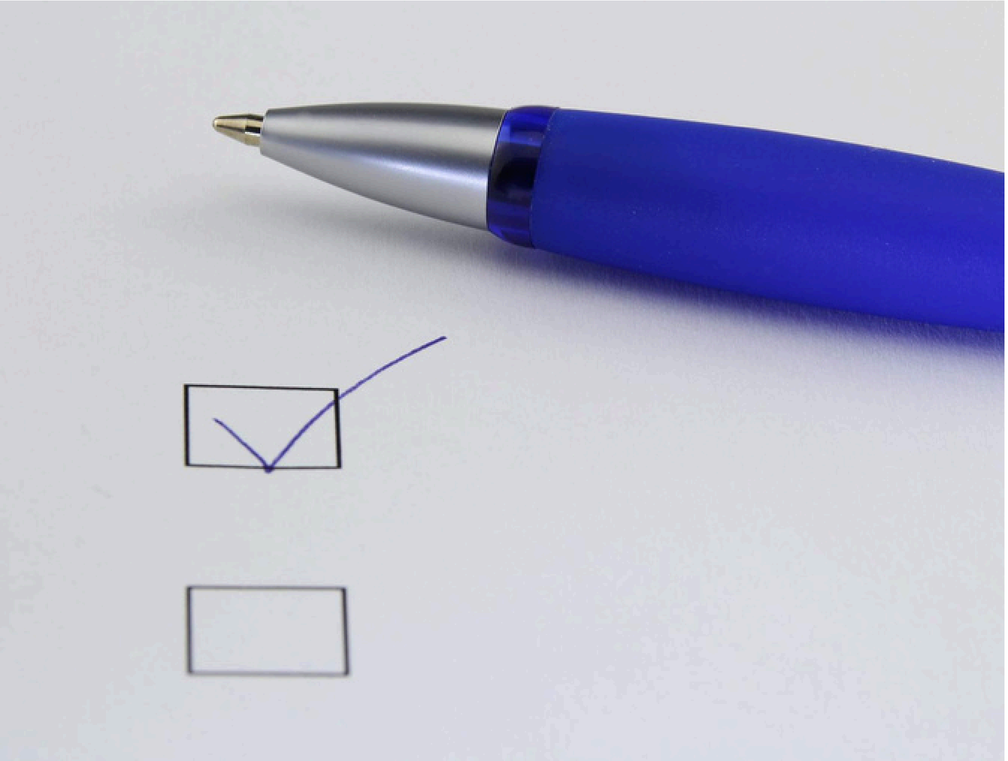
Tip 4

Add Length



The longer the better, although not so long that you forget it. Some IT people recommend a minimum of 8 characters; many others would say 10.

Summary



Remember:

- Your password should consist of a mixture of upper and lower case letters, special characters such as '*' or '!', and should be of a minimum length of 8- 10 characters.
- Do not use a password consisting of letters only
- Do not use a password consisting of numbers only
- Do not base your password on well known words or phrases
- Do not base your password on information you post on social networking sites

Best Practice

□ Your password should be based on a mixture of upper- and lower-case letters, special characters and numbers, and be of a minimum length of 8-10 characters.

□ Change your password at regular intervals, typically every 90 days.

□ Don't base your password on well-known phrases or number s equences .

□ Don't base your password on information that is known about you - name, address, phone numbers, favorite teams, children's names etc.

□ Don't share your password with anyone, not even close colleagues, friends or family members.

□ Never write down your password - memorize it.

□ Don't send your password in an email.

Thanks for completing this course!

Visit our website www.vigitrust.com

Email: info@vigitrust.com

VIGITRUST