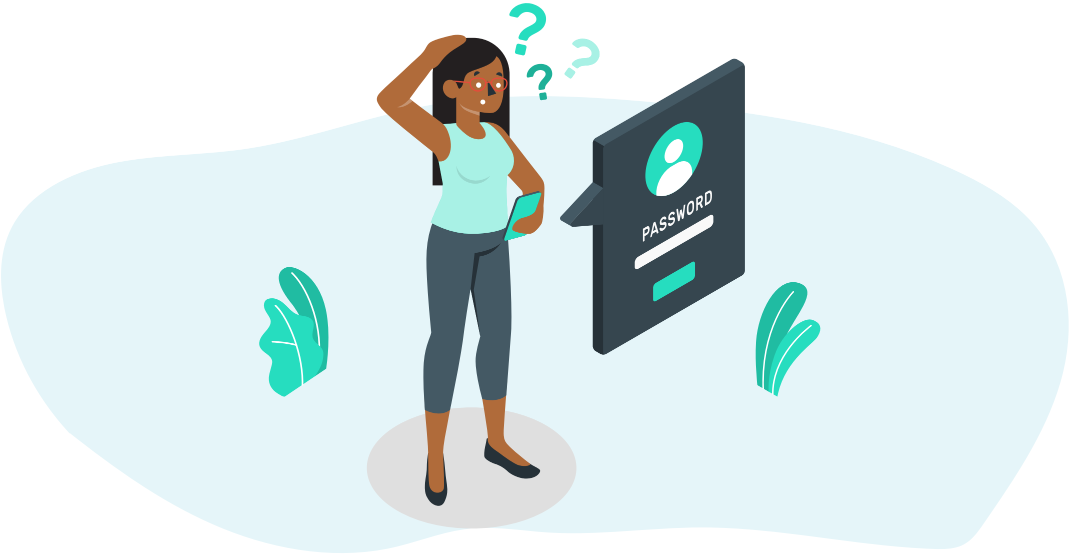
CYBER CRIMINALS AND YOUR PASSWORD

What They Do And How They Get To It

A key is to a door, what passwords are to our prized information and assets.



What is a Password?

Passwords are virtual keys made up of either numbers, letters, symbols, or a combination of all of the above. They are used to authenticate the identity of a person seeking access to an online asset like a social media account, website, or an electronic device.

But passwords do not work alone. Just like a tag team, passwords are always paired with user-names.

Knock, Knock

Who's there?

Amaka, the owner of this account?

Well, where's your key?

If passwords are keys and i never share mine,

How do bad guys steal it?

Short answer, by cracking them. Smash, smash! Not what you were expecting huh? Sadly, although passwords are neither kernels nor coconuts, they can be cracked.

How?

Before answering how let's define password cracking.

What is Password Cracking?

Password cracking is a technique unauthorized users (cybercriminals), use to fish out the password set as protection for an account, computing device, or digital asset. Once, this is done they pretty much have full control over that account and proceed to make a nuisance of themselves.

To help you better understand how hackers get your passwords, here's a list of the most popular password-cracking techniques used across the internet.

Guessing

This is what hackers do until they land on the right password to your account. Well, maybe not so literally.... But you get the point.

This technique works because cybercriminals know most individuals go with what's familiar or important when creating passwords. So, your passwords are most likely to be based upon interests, significant dates, nicknames, hobbies, pets, family, and so on.

The bad guys gain access to this information (which is often in abundance on your social media accounts) and make guesses of what your password could be.

And boy, do they get it right more times than not!

Shoulder Surfing

Look away, you thief!

A little seemingly harmless side glance or peek over your shoulder is sometimes all a hacker needs to steal your personal identification numbers (PINs), passwords, and other confidential information.

Shoulder surfing can happen when you enter personal information in public. For example, at the ATM machines, payment kiosks, and more. It is simple really when keypad and touchscreen entries can be watched, do not put in your personal information!

Brute Force Attack

Now, this is where the big guns come out.

With this technique, the hacker uses an automated software that tries multiple combinations of letters, numbers, and special characters until a password match is found. It is relentlessly, going for the most used passwords first. With this software, weak or common passwords become relatively simple for the hacker to crack. Cue in - "admin123". Yes, it is that easy. Just like taking candy from a baby.

Dictionary Attack

The dictionary attack is the less-sophisticated sister of the brute force attack, it relies on hackers bombarding a system with guesses until something sticks. But unlike the brute force attack where the guesses are random, the hacker relies on an index of words that are often used as passwords.

Social Engineering

Picture this, you can see and smell a slice of cheesy gooey pizza; just when you open your mouth to grab a bite, the person who offered to feed you the pizza, pulls it back and inserts a bitter vegetable into your mouth... Yuck!

This is exactly what social engineering is, the art of manipulating and deceiving a victim into divulging sensitive or confidential information e.g. bank information, passwords, etc.

Phishing, Vishing & Smishing

Phishing, Vishing, and Smishing are all fruits from the same tree - social engineering. What differentiates one from the other is the channel they are used on:

Email = Phishing
Phone = Vishing
SMS = Smishing

However, regardless of the channel, one thing is constant, the hacker will impersonate a person or organization you trust in order to obtain sensitive information such as your identification information, financial/banking details, and passwords.

Rainbow Table Attack

Did you know, passwords are stored using encryptions? That's right, unlike this text you are reading, they are typically stored using a crazy looking chain of characters called hashes. For instance, a password like "pumpkin22" after hashing could look like this “614B1F421A1F5272FF72A13CAC74F56".

At this point, you are probably wondering what any of this has to do with password cracking. Well, when hackers steal a file containing hashed passwords, they use a Rainbow Table attack to decode the passwords.

How does this work? A Rainbow Table is a dictionary or table that has been enhanced to decipher password hashes. It works by comparing every known hash value, against hashes found in a stolen passwords file, looking for a match.

In simpler terms, the Rainbow table attack is the rich cousin of brute force attack, he drives a Lamborghini and travels to Italy to eat 'authentic' Pizza. Good for him, but bad for the environment. Avoid him at all costs.

Malware

A favourite among Cyber Criminals!

Malware is not a man of peace, he is a warrior, he is a fighter, he is the indabosky bahosa! Can somebody scream Spartan?!

Okay, on a serious note, Malware is a lethal software used for the sole purpose of gaining unapproved access to a computer system. In most instances, it is delivered in the form of a link or file via email.

It remains dormant until you click on the link or open the file, and then like Pandora's Box unleashes unspeakable horrors unto your computer.

A malware attack can also infect your computing device from harmful ads that have been planted by a hacker on naughty websites. So, on your next visit to you-know-where, avoid clicking on ads.

Spidering

Spidering is the most intimate technique on this list.

The hacker begins by getting to know you intimately, through web digging(information research). It is important to note, a spidering attack is often targeted at organizations. Why? The answer lies in the availability of ready information. A lot of organizations use corporate passwords that relate to their business in some way; for example, using a variation of their brand name as the password for their Wi-Fi network.

"Good" hackers have realized that by studying a business' corporate literature, whether it's the company's mission statement or their sales material, they can build a highly effective word file that can be used as part of a carefully planned attack. If you run a business with an online presence(who doesn't these days), **consider hiring a cybersecurity expert now**. After all, better safe than sorry, right?

Steal Password from Browser

Most web browsers offer password storage after you login to a service. If you accept, your password is stored on the browser. Hence, one of the first things a cybercriminal does after hacking a device is to search for browser passwords. Think about it, the best place to look for something valuable is in a safe. Nobody knows this better than the cybercriminal.

ONE LAST THING

Now that you know what cybercriminals do to get at your passwords, it is time to beef up your security measures. Not to worry, everything you need to know will be covered in our follow up piece. While you wait, you can find other juicy cybersecurity tips and tricks for free on our social media pages:

@nogofallmaga

@nogofallmaga

@nogofallmaga

www.nogofallmaga.org
www.cybersafefoundation.org

CONTRIBUTORS

Wale Osoba
John Ajayi
Teslimat Okanlawon
Enyinna Abazie
Designer: Daniel Emenahor
Content Writer : Michelle Etiuwa Umobong
Curator: Confidence Staveley