




A. GOPALA KRISHNA

**BE
A
CYBER
WARRIOR**

BEWARE OF CYBER CRIMES

Everything is connected,
Everyone is dependent,
How to survive?



Copyright © 2019, A. Gopala Krishna
All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording or any information storage and retrieval system now known or to be invented, without permission in writing from the publisher, except by a reviewer who wishes to quote brief passages in connection with a review written for inclusion in a magazine, newspaper or broadcast.

Published in India by Prowess Publishing,
YRK Towers, Thadikara Swamy Koil St, Alandur, Chennai,
Tamil Nadu 600016

ISBN-10: 1-5457-4353-3

ISBN-13: 978-1-5457-4353-9

ePUB ISBN: 978-1-5457-4354-6

Mobi ISBN: 978-1-5457-4355-3

Library of Congress Cataloging in Publication

Contents

Preface

Acknowledgment

About the Author

1. Your password is an entry to your digital life
2. Securing Operating Systems
3. Smartphones safety
4. Stay safe on Social media
5. Digital Payments
6. Online frauds
7. Children safety
8. Securing from Malware
9. You're not the customer you're the product
10. Don't leave your digital footprints
11. Be a hacker with ethics

References

CHAPTER 1

Your password is an entry to your digital life

“For every lock, there is someone out there trying to pick it or break in”

—DAVID BERNSTEIN

Introduction

Millions of people use online services every day for simplifying their needs, like composing an office Email, carrying out Bank Transactions, navigating to a road trip, online tutorials, reading blog articles, chatting with friends, watching movies, shows, order food online & booking a cab; So we mostly rely on online services to meet our daily needs.

You need to log in to the specific website to experience their web services. To log in to a site, you have to confirm your identity with the login credentials (username & password) that you have registered with the site while signing up for an account. Usernames & passwords are the most common ways of authenticating and play an essential role in our digital life.

What would ensue if your Facebook account got hacked, criminals could use this compromised account to put you in trouble, they may blackmail you with sensitive information like personal photos and messages found on your account. A cybercriminal can use your Facebook account to abuse, someone, on behalf of your name, malicious hackers can post irrelevant and controversial political statements to spoil your reputation. Hacking your Facebook account may not affect you financially but damages your profile and reputation socially. What if the login details used for Facebook and online banking are the same? you're the one making paths for cybercriminals to harm your digital life. It doesn't sound good right that's why it is essential to preserve your passwords.

Compromising your Facebook or Google Accounts is not the end goal for cybercriminals, It's just the beginning. Because 60% of people use the same usernames and passwords across multiple websites, same passwords for Facebook, Online banking and brokerage accounts, if any one of the accounts reports compromised (Hacked), another web service using same login details can also easily compromised.

The objective of this chapter

This lesson would explain how password functions in real time, and how to create a strong password, how to use Two-factor verification, what is the alternative to passwords, and use of Password managers.

Case studies:

Cybercriminals have lost no time in taking advantage of technology to ruin your digital life; these are the most significant data breaches reported in history, the technologies that we rely on every day also got compromised.

- Facebook reported a data breach on Sep 2018 where 50 million user accounts got compromised (Hacked).
- LinkedIn reported a data breach on June 2012 where 6.5 million user accounts got stolen by Russian hackers.
- Snapchat reported a data breach in 2013 where 4.6 million user accounts got compromised.
- Yahoo reported a data breach in 2013 where 200 million user accounts got compromised, reported as most massive data breach ever in the history.
- Adobe reported a data breach in October 2013 where 38 million user accounts got compromised.
- Sony PlayStation reported a data breach in June 2011 where 72 million user accounts compromised along with the credit card numbers and contact numbers.
- Uber reported a data breach in 2016 where 57 million customers and driver's data got compromised.
- Rock You games Online Gaming company reported a data breach in 2009 where 32 million user accounts got compromised (**Source: [Wikipedia.org](https://en.wikipedia.org/wiki/Rock_You_games)**)

The information stated above is to convey to the users that, how securing information is a challenging task in this growing technological era. The information specified above is for an educational purpose not to spoil the reputation of any technology. By looking at the above records one should ask themselves, the data you're producing and storing daily in your smartphones, desktops, and cloud services, are they secure? How much secure enough your data is? And what kind of security measures you are taking to protect data against cybercriminals.

Giant organizations stated above take various security measures and implement many security policies to safeguard organizational and users data

from cybercriminals. But due to unknown vulnerabilities (weakness) in the hardware and software make them prone to cyber attacks, but technological organizations quickly recover from the cyber attacks and continue their business & services without interrupting the users.

The fact is; In cyberspace with enough time, energy, and attention along with resources any system can be hacked, but by implementing some security measures and security policies, we can add an extra layer of security to safeguard data from cybercriminals.

How password functions

When a user enters a password, it is verified against the passwords saved in the website. If the password matches, the user is granted to access the account.

Websites don't store the password in plain text, instead use hashing algorithms (MD5, SHA) to protect from cybercriminals. Hashing is used to create one-way encrypted text that can never be decrypted. Hash values play a vital role in importing the integrity of the data. When you enter your password on a website, it simply performs the hashing for password and checks the result against the hashes stored on a database and verifying the validity of the password without having to store the sensitive password itself.

How Plain text looks when converted to a Hash value

Plain text – Hello this is Hacker

Hashed Value for above text –
84218b9b8ba3b8d5351064fe97495a61

Website stores hashed values, instead of plain text to safeguard information in case Data Breaches.

How hackers break passwords:

We can prevent hackers from cracking our passwords by knowing how passwords can be compromised, only then we can learn how to create a strong password.

Method 1

Hackers try to obtain more information about you through social media, like your first name, last name and about your family, contact information, your favorite music album, your favorite sports team, and your pet name. Cybercriminals use this piece of information to crack your passwords, in this stage, there is a 40% of chance that a password can be cracked because most

of the people use passwords with their personal information, this makes user passwords vulnerable to attacks. So, don't use passwords that relate to your personal information.

Method 2 (Dictionary attack)

In this method, hackers use a dictionary attack, where a set of commonly used default passwords are listed in a ".txt file", e.g: "1234" "abc123" "admin" "pa\$\$word" "I love you" "qwerty" "adobe123" "iamking" etc..., where the most of internet users rely on such kind of default passwords which are easily hackable. Cybercriminals use tools to automate their work. The script engine is used to compare the list of default password hashes from dictionary file with the stored database of passwords hashes of a website, the script tries one after another of all the several default passwords from the list until it found the same hash. When both password hashes get matched, the hacker can get access into the account. So don't use default passwords, instead create a strong password.

Method 3 (Brute force attack)

In this method, hackers use a crunch tool to generates a password file with a combination of Alphabets, Numbers, and Symbols and store all several random combinations in a ".txt file."

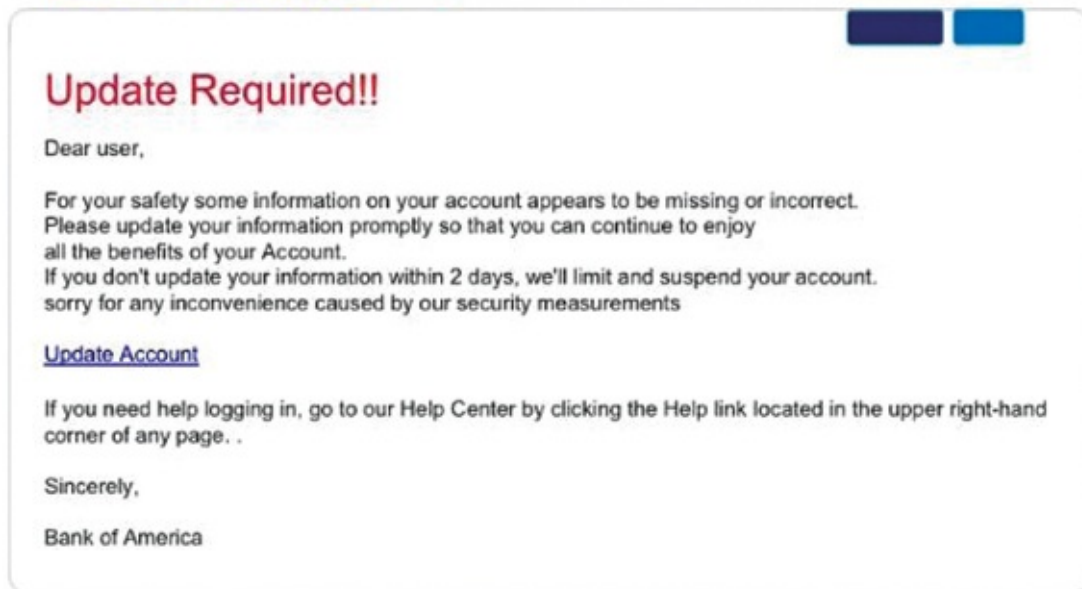
Cybercriminals use tools to automate their work. The script engine compares the list of several combinations of the password from the text file with the stored database of password hashes of the website, the script tries to compare one after another password in the password list until password hashes match. Hacker can get access to accounts if password hash is matched, even though Brute force attack takes time, but the success rate is high.

To prevent brute force attacks, use a combinational and long password ranging from 15–20 characters, which would take several years to crack using brute force attack.

Method 4 (Keylogger attack)

If a keylogger is installed into your computer, it can capture all your keystroke that you type on your keyboard. Most of the time cybercriminals infect your system with backdoor which has sub-function of keylogging, at the end of the day, the user typed keystrokes including username and passwords are also recorded and sent to the hacker. So to prevent a keylogger from infecting your PC use a premium anti-virus. It is advised not to enter any sensitive information in public pc or friend's pc because they may record all your keystrokes with keyloggers.

Method 5 (Social Engineering attacks)



(Image Source: <https://tech.co/top-6-online-scams-avoid-2018-08>)

Cybercriminals send phishing emails to get your login credentials. Look at the above screenshot of a phishing email that duped as it came from the bank of America asking to update user details; this is an example of how malicious hackers fool humans to get what they want, don't blindly click on those links to update your account details; they are created by cybercriminals to gain access to your bank username and passwords. When you blindly click on those links in the email, you will come to land on the banking website that looks like your banking, but it is a phishing page of your original bank website. If you blindly give your username and passwords on that fake web page, hackers would capture your login details and make transactions with your money, such type of attack is called phishing attacks.

In case if you receive emails asking you to change the password or asking you to update your account details just ignore them and report them as spam. Because any banks don't send such kind of emails to its customers. Don't fall victim of Phishing attacks beware of them.

Pick a strong password

A string of Alphanumeric characters can no longer protect you; you might set a time for creating a strong password.

What can be the strong password?

A password that doesn't relate to your personal details and doesn't contain dictionary words and default passwords which are easily guessable. Your

account will be more secure enough; only when you use 12–20 characters long password with a combination of upper case & lower case letters along with numbers and symbols, with such random combinations a password can be referred as a strong password, it is advisable to maintain different passwords for different websites.

Example of strong passwords

1. Yk&joR58KrpFvD\$%689
2. LRnUvC5678%\$#KpO367

Although the above password is long and unique enough and more secure, it is arduous to recall when necessary, to overcome such problem learn to use a passphrase.

Passphrase

The passphrase is similar to a password in usage; a passphrase is constructed using a sentence which is long and unique enough and can recall when necessary. Often passphrase is used instead of password managers to remember the complex passwords.

Examples of passphrase:

@ppleFoUnDbY\$teveIn1976 -
apple found by Steve in 1976(a=@,S=\$)

@oHjEniFeR!\$100%cUtE -
@OH JENIFER IS 100% CUTE (I=!)

#WhOsEcAtEgOrY10/10fOnTsMaTcH -
#WHOSE CATEGORY 10/10 FONTS MATCH

Above passphrase satisfy the requirement of a strong password

1. Memorable enough that user can recall it without writing down.
2. Unique and Long enough that no one else can guess it.

The second layer of security:

1. Two-factor authentication

If passwords are not secure enough, perhaps having two pieces of information is more secure, two pieces of information include your username & password (something you know) and one-time password (something you have). Most consumer internet companies, banks use your smartphones as the second factor of authentication by sending you a six-digit code via text message that

you must also enter to gain access to your account. Two-factor authentication ensures you're the only one who can access your accounts, even if someone knows your password.

What is Two-factor authentication?

As it pronounced, Two-factor authentication requires two pieces of information to be verified, to get access to your user account.

Example: The usage of Two-factor authentication, while online banking transaction, you have to provide two pieces of information to the bank.

1. The Username and Password (Something you know).
2. You have to enter OTP sent to your mobile (Something you have).

When these two factors match with the bank database, then you're allowed to withdraw money. Otherwise, you cannot get access.

Some companies like Google, Facebook, Apple, Microsoft Supports Two-factor authentication, to provide an extra layer of security to their users. A user needs to enter two pieces of information rather than a single password to access his/her profile.

When signing to a web service a user needs to log in with the username and passwords (something you know) along with the OTP sent to the registered mobile number of the user (something you have) to validate the login. So, if hacker learned to get your password, he could not access your account without the OTP message.

The pattern of Two-factor authentication:

1. Something you know
2. Something you have

How to turn on Two-factor Authentication

Two-factor Authentication for Google

1. Login to your **Gmail**
2. Navigate to **Google Account** by clicking on the top right corner of your profile picture.
3. Go to the Security tab
4. Find **signing in to Google tab** and click on 2-Step Verification.
5. **Click** on get started
6. **Turn on** 2-step verification

Two-factor Authentication for **Facebook**

1. Login to **Facebook**
2. Go to settings by clicking on the ▼ button at the top right corner of Facebook and click on **Settings > Security and Login**
3. Scroll down to use **two-factor authentication** and click **Edit**
4. Choose the authenticate method that you want to add and follow on-screen instructions
5. Click **Enable** once you have selected and turned on the authentication method.

2. Authenticator apps:

Google and Microsoft provide authenticator apps on their respective app stores where a code containing six digits is issued to the mobile apps from the mainframe computer of Google and Microsoft, which can be expired within one minute and generates new six-digit code for every minute to the mobile user app to ensure the confidentiality of information.

Try out **Google Authenticator** and **Microsoft Authenticator** available on Play store and App store.

3. Biometric Authentication

Bio-metrics play an essential role from unlocking the device, making digital payments on-the-go. Biometrics (fingerprint, facial recognition & Iris scan) provide better security compared to Passwords and passcodes. Passwords should be memorable to recall when necessary and there is a fair chance of forgetting them, but your fingers and your face is always with you never worry about forgetting passwords again.

#Your face is your password

(Source: Apple)

4. Password managers

Maintaining different passwords for different websites is good practice of security implementation, but at last, we end up with confusion, so to end this confusion. Security expert's best advice is to use password managers.

Using password managers we can save our login credentials of various web services at one place (one master password to all your login credentials), the stored login credentials are encrypted by default and protected with a username and the master key. Password managers are harder to crack; Password managers provide both mobile and desktop version of their applications so we can access password managers from any device and

anywhere, better ensure a strong master password while using password managers.

No need to worry about forgetting passwords again. With the help of password managers, we can generate new strong passwords with its built-in password generator tool.

Password managers: LastPass, Dashlane, 1 password, KeePass.

Password salting

Most of the websites use salting method, in which random characters are added to the password before it's been hashed. Do remember salts are added automatically after the user enters username and password. A particular website uses random characters of a particular type in salting. Although malicious hacker got access to vulnerable login credentials database, he cannot crack the salted passwords until he is aware of the random data used in the process of salting. Only website and database know which random data should be added while salting. So salted password hashes are difficult to crack.

Countermeasures to secure from Cyberattacks:

Things to implement:

1. Use strong passwords

A Passwords can be secure only if it doesn't contain personal information and dictionary words which are easily guessable; a strong password is like long and unique enough with a combination of alphabets (upper case & lower case), numbers and symbols. and the password should be range from 12–20 characters.

2. Pick a unique username

Don't pick a username that points back to your personal information, (Especially for net banking) don't use the combination of your names and phone numbers or vehicle registration numbers for as usernames. They will be easily guessable by looking at your social media profiles, instead, use random usernames rather than your phone numbers or first name and last name or vehicle registration numbers, pick a Good & Strong username.

3. Periodically change passwords

Not all the hackers take what they need. Occasionally hackers may continue to spy for stealing information over time without your knowledge, to keep pull stop to such incidents, it is advisable to change your password on a frequent basis at least for a month to be more secure.

4. Clear browser cookies

A website inserts cookies into user web browsers when the user visits the site for the first time. Browser cookies are used to store data of the corresponding website according to user preference and user details, such as user login details, language preferred by the user for the site and site layout and the items stored by the user on his shopping cart. Data stored on the cookies is used when a user revisits the same website next time, site modifies the website content according to user preference and logs user automatically by retrieving data from browser cookies. Sometimes Hacker can steal your browser cookies to access your accounts.

So, it is advisable to clear your browser cookies after web surfing, to safeguard from such cookie stealing cyber-attacks.

To auto clear your cookies in Google Chrome

Settings > Scroll down and expand **Advanced Menu** > **Content setting** > **Cookies** > **Turn on** Keep local data until you quit the browser.

5. Use Two-factor Authentication

If your passwords are stolen by hackers anyhow, they cannot access your account without the OTP, that can be only sent to the registered user mobile, two-factor authentication provides you confidentiality of information. Turn on two-factor authentication for your web services now.

Authenticator apps: Google, Microsoft, LastPass Authenticator.

6. Password managers

In password manager, you can save all your login credentials at one place which are encrypted by default. Logging with username and master password provides access to the stored password's. So no worries about forgetting passwords again.

Password managers: LastPass, Dashlane, 1 password, KeePass.

7. Use Biometrics

Biometrics (fingerprint facial recognition & Iris scan) provide better security compared to Passwords and passcodes. Most of them use fingerprints and face ID to unlock the device, to make payments.

8. OAuth login

OAuth (open authorization) login provides access tokens, with the help of OAuth login, users can use Google and Facebook login details across the internet to login to any third party website, without signing up for a new account. This is called single sign-on.

9. Configure Back up phone number & Back up Email

Always configure backup email and phone number to your emails and social networking sites, to retrieve the forgotten passwords and to get alerts of suspicious activity (if some unauthorized person had access to your account) on your email or social network accounts.

10. Security Questions & hints

Security questions and hints are helpful in retrieving the forgotten passwords. Set strong & hard to guess security questions and answers.

11. Mobile phone & Desktops passcodes

The whole information stored on your mobile/laptop is protected with the password/pin from unauthorized access, as weak passwords always put you in trouble, never use four digits pin to unlock the device, at least use 6–8 digit pin to unlock the device.

12. Check for HTTPS

When logging to any website, look at **https://** (“Hypertext Transfer Protocol Secure”) with a padlock symbol. Because logging from sites which use **http://** is not secure; hackers may intercept and steal the login credentials from **http://sites**, It’s advisable only to log into a web service which uses **https://protocol** with a padlock symbol.

https:// websites use **SSL** certificate which allows us to secure connection by encrypting the data between server and client. Hackers cannot intercept the data because the data is encrypted. Always look at **https://** with padlock symbol in the URL while logging to any website.

13. Virtual keyboards

When logging from public computers/shared Pc’s/Libraries, log in with virtual keyboards, because someone can record all your keystrokes using keyloggers in public/shared computers, so better to use virtual keyboards when logging from public computers. Never forget to log out from those computers which don’t belong to you.

Things not to do:

1. Prevent use of easily guessable passwords

Don’t use passwords that relate to your personal information like first name and last name and family member names, contact details, the city you live, your pet name. Because if a hacker tries to gather information about you through social media, the passwords can be cracked easily, try to not use your personal information in passwords, and don’t use default passwords like

admin, password, 12345, iloveyou, abc12345, qwerty, adobe123, etc....

Hackers use a dictionary attack to crack default passwords. Prevent the use of default passwords, use a strong password ranging 12–20 characters long with the combination of uppercase, lowercase, numbers, and symbols.

2. Prevent reuse of passwords

If you are still using the same password for all your online accounts, then your digital life can be ruined in a matter of seconds. If you use the same password for our online banking and Facebook, if your Facebook account is compromised then your online banking account can also get compromised, to prevent reuse of passwords, try password managers (password managers use encrypted passwords and protect them with a master key), to maintain different passwords for different websites.

3. Don't write down passwords in a sticky note

Many of them write passwords in the sticky note and keep them near to computer desk either in home/office if anyone who has physical access to your computer desk can find login details which can be misused, so never write down passwords and keep near to your computer desk.

4. Don't fall, victims of social engineering attacks

If you got an email from your bank to “change the password immediately by clicking on the below link”, don't blindly click on the link to change passwords, because they are created by cybercriminals to get access to your bank username and passwords.

When you blindly click on those links, you will come to land on the banking website that looks same as original site but it is a duplicate of your original bank website. If you blindly give your username and passwords on that fake web page, hackers can capture your details and make transactions with your money, this type of attack is called phishing attack.

Try to ignore such type of emails asking you to change the password. Please don't fall victim of Phishing attacks be aware of them.

5. Don't save passwords into the browsers

Don't allow autosave of passwords when browser promotes you to do. Because the passwords saved in browsers are not encrypted, they can be easily viewed/misused by anyone who has accesses to your computers, so do not click on Remember passwords when your browser prompt an autosave passwords window.

6. Don't log into a website that uses HTTP protocol

http://site don't encrypt the data when login details are passed from client to server, so they can be captured by anyone who is in the same network and passwords can be easily stolen. Use https://protocol websites which use SSL certificates that encrypt the data.

Summary

In this lesson, we have seen most significant data breaches in the technologies, how password functions, how hackers hack your passwords, difference between weak passwords and strong passwords, learn to create a strong passwords and passphrases, importance and use of using Two-factor authentication, and use of password managers, and biometrics, finally the countermeasures to be followed to mitigate the password attacks.

Conclusion

Any system cannot be 100% hackproof, with enough attention, time and energy along with resources any system can be compromised, our goal is to mitigate the chances of cyber threats by following security policies and procedures.

Create your strong password today to have a safe and secure digital life tomorrow.

You've Just Finished your Free Sample

Enjoyed the preview?

Buy: <http://www.ebooks2go.com>