



Cybersecurity for Everyone

A Beginner's Guide to Staying Safe Online

Version 1.0

Created by
Deepak Webcrafts

Disclaimer

This ebook is created for educational and awareness purposes only.

It does not teach hacking, unauthorized access, or any illegal activities.

The information provided is intended to help readers improve their personal cybersecurity and stay safe online.

The author is not responsible for any misuse of the information contained in this ebook.

Table of Contents

1. Introduction to Cybersecurity

What is Cybersecurity? | Why everyone needs it | Common cyber threats

2. Password Security

Strong passwords | Common mistakes | Password tips | Password manager

3. Mobile Security

Safe app downloads | App permissions | Phone updates | Screen lock

4. Internet Safety

HTTPS | Fake websites | Safe browsing | Public Wi-Fi | Safe downloads

5. Social Media Safety

Instagram safety | WhatsApp privacy | Facebook basics | Oversharing

6. Scam Awareness

OTP scams | UPI scams | QR code scams | Fake customer care | Phishing

7. Banking & Payment Safety

Online banking tips | Card safety | Payment precautions

8. If You Get Hacked

Gmail hacked | Instagram hacked | Lost phone | Immediate actions

9. Daily Cyber Habits

Daily checklist | Weekly checklist | Golden Rules

10. Cybersecurity Glossary

Simple meanings of essential cybersecurity terms

Chapter 1

Introduction to Cybersecurity

What is Cybersecurity?

Cybersecurity is the practice of protecting computers, smartphones, online accounts, networks, and personal information from cyber threats such as hackers, scammers, malware, and data theft.

In simple words, cybersecurity means keeping your digital life safe. Just as you lock your house to prevent theft, cybersecurity protects your online world from unauthorized access.

Today, almost everyone uses the internet for communication, shopping, banking, education, and entertainment. Because so much of our personal information is stored online, learning basic cybersecurity has become an essential life skill. Cybersecurity is not only for IT professionals or large companies—it is important for every internet user.



Pro Tip

Protecting your digital identity is just as important as protecting your physical identity.

Why Does Everyone Need Cybersecurity?

Every day, millions of people receive fake messages, scam phone calls, phishing emails, and malicious links. Many lose access to their accounts or even their money simply because they were unaware of basic online safety practices.

Whether you are a student, employee, business owner, parent, or retiree, understanding cybersecurity can help you:

- Protect your personal information
- Keep your online accounts secure
- Prevent financial fraud
- Avoid online scams
- Use the internet with confidence

Cybersecurity awareness is no longer optional. It is a necessity in today's digital world.

Common Cyber Threats

Phishing

Phishing is an attempt to trick people into revealing sensitive information such as passwords, OTPs, or banking details through fake emails, messages, or websites.

Malware

Malware is harmful software designed to damage a device, steal information, or monitor user activity. Examples include viruses, worms, spyware, and ransomware.

Identity Theft

Identity theft occurs when someone steals your personal information and uses it without your permission. This information may include your name, email address, phone number, Aadhaar details, or banking information.

Password Attacks

Weak or reused passwords make it easier for attackers to access your accounts. Using strong and unique passwords significantly improves your security.

Online Scams

Scammers often pretend to be banks, delivery companies, customer support agents, or government officials to steal money or personal information. Always verify before trusting anyone online.

Your Digital Identity

Your digital identity is the collection of information that represents you on the internet. It includes:

- Email accounts
- Social media profiles
- Mobile number
- Passwords
- Online banking accounts
- Shopping accounts
- Photos and documents stored online

Protecting your digital identity should be one of your highest priorities because losing control of it can affect both your privacy and finances.

Key Takeaways

- ☐ Cybersecurity protects your digital life.
- ☐ Every internet user should understand basic cybersecurity.
- ☐ Hackers and scammers often target ordinary people.
- ☐ Strong security habits can prevent most online attacks.

Quick Quiz

1. What is the main purpose of cybersecurity?

- ☐ A. Speed up the internet
- ☐ B. Protect devices and personal information
- ☐ C. Increase mobile storage
- ☐ D. Improve gaming performance

Answer: B

2. Which of the following is considered part of your digital identity?

- ☐ A. Email account
- ☐ B. Social media profile
- ☐ C. Bank account
- ☐ D. All of the above

Answer: D

3. True or False: Cybersecurity is only important for large companies.

Answer: False

Chapter 2

Password Security

Why Are Passwords Important?

A password is the first layer of security for your online accounts. Whenever you log in to your email, social media, banking app, or any website, your password helps verify your identity.

If someone knows your password, they may gain access to your personal information, private conversations, photos, documents, or even your money. A strong password is one of the easiest and most effective ways to protect yourself online.

What Makes a Strong Password?

- At least 12–16 characters long
- A mix of uppercase and lowercase letters
- Include numbers
- Include special characters (such as @, #, \$, %, &)
- Difficult to guess
- Unique for every important account

✗ Weak Passwords

12345678
password
qwerty123
deepak123
iloveyou

✓ Strong Passwords

Dk@2026#Moon!
C0ffee&Sunrise24
MyBike\$Runs@Fast9

Common Password Mistakes

Many people unknowingly make simple mistakes that put their accounts at risk. Avoid these habits:

- Using your name as a password
- Using your date of birth
- Using your mobile number
- Using the same password everywhere
- Sharing passwords with friends
- Writing passwords on paper where others can see them

⚠ Warning: Credential Stuffing

If you use the same password for Gmail, Instagram, and Banking, a data breach on one site means attackers can access ALL your accounts. Never reuse passwords.

Use Passphrases Instead of Short Passwords

A passphrase is a long, memorable sentence used as a password.

Example: **Coffee!Morning2026Sun**

Passphrases are easier to remember and much harder to crack than short passwords.

What Is a Password Manager?

Remembering dozens of unique passwords can be difficult. A password manager is an application that securely stores your passwords in one protected place. You only need to remember one strong master password. Many password managers can also generate strong passwords automatically.

Change Passwords When Necessary

You do not need to change your password every month without a reason. However, change it immediately if:

- You shared it with someone.
- You suspect your account was hacked.
- You notice unusual login activity.
- A website reports a security breach.

Quick Quiz

1. Which password is the strongest?

- ☐ A. 12345678
- ☐ B. deepak123
- ☐ C. Dk@2026#Moon!
- ☐ D. password

Answer: C

2. Why should you avoid using the same password for multiple accounts?

- ☐ A. It wastes time.
- ☐ B. It makes accounts easier to remember.
- ☐ C. If one account is compromised, others may also be at risk.
- ☐ D. There is no reason.

Answer: C

Remember

Your password is like the key to your house. If you wouldn't hand your house key to a stranger, don't share your password with anyone.

Chapter 3

Mobile Security

Why Is Mobile Security Important?

Today, your smartphone contains more personal information than your wallet. It stores banking apps, UPI apps, photos, emails, social media accounts, and saved passwords. If your phone is lost, stolen, or infected with malicious software, your personal information could be exposed.

Always Lock Your Phone

A screen lock is your first line of defense. Choose one of the following:

- PIN
- Password
- Fingerprint
- Face Unlock

A strong PIN or password offers better protection than simple patterns. Avoid easy combinations like 1234, 0000, or your birth year.

Keep Your Phone Updated

Software updates do more than add new features. They also fix security vulnerabilities that attackers may try to exploit. Whenever your phone asks for a security update, install it as soon as possible.

Download Apps Only from Trusted Sources

Always install applications from official app stores (Google Play Store for Android, Apple App Store for iPhone). Avoid downloading APK files or apps from random websites.

Review App Permissions

Some apps ask for permissions they don't actually need. For example, a calculator app should not need Camera access, Contacts, Microphone, or Location.

Always ask yourself: *"Does this app really need this permission?"* If the answer is no, deny the permission whenever possible.

Avoid Rooting or Jailbreaking

Some users modify their phones to gain extra control (Rooting for Android, Jailbreaking for iPhone). While it offers additional customization, it also removes important security protections.

Use Trusted Wi-Fi Networks

Public Wi-Fi is convenient but not always secure. Avoid using public networks for internet banking, UPI payments, password changes, or accessing sensitive accounts.

✓ Mobile Security Checklist

- ☐ Use a strong screen lock.
- ☐ Keep your phone updated.
- ☐ Install apps only from official stores.
- ☐ Review app permissions.
- ☐ Enable Find My Device.
- ☐ Back up important data regularly.

Quick Quiz

1. Where should you download apps from?

- ☐ A. Random websites
- ☐ B. Messaging apps
- ☐ C. Official app stores

Answer: C

Chapter 4

Internet Safety

What Is Safe Browsing?

Safe browsing means using the internet in a way that protects your personal information, devices, and online accounts from cyber threats. Every website you visit and every link you click can either keep you safe or expose you to risks.

Check the Website Address

Before entering any personal information, always check the website's address (URL).

- ✓ Official: <https://amazon.in>
- ✗ Fake: <https://amaz0n-in.xyz>

Notice how a small change in spelling can make a fake website look genuine. Cybercriminals often create websites that closely resemble trusted brands to trick users.

What Is HTTPS?

Most secure websites begin with **https://**. The "S" stands for Secure. HTTPS encrypts the data exchanged between your device and the website.

⚠ Important Notice

HTTPS does not guarantee that a website is legitimate. Scammers can also create fake websites that use HTTPS. Always verify the domain name itself.

Think Before You Click

Cybercriminals often rely on curiosity and urgency. Be cautious if you receive messages such as:

- "Congratulations! You won a prize."
- "Your account has been suspended."
- "Verify your KYC immediately."

Avoid Sharing Personal Information

Never enter personal information on websites unless you trust them. Sensitive information includes Passwords, OTPs, Aadhaar Number, PAN Number, Bank Account Details, Debit/Credit Card Information, CVV, and UPI PIN.

Legitimate organizations will never ask for your password or UPI PIN through a website, message, or phone call.

Internet Safety Checklist

- ☐ Verify website addresses.
- ☐ Look for HTTPS.
- ☐ Avoid suspicious links.
- ☐ Ignore fake pop-ups.
- ☐ Never share sensitive info on unknown sites.
- ☐ Log out from shared computers.

Chapter 5

Social Media Safety

Why Is Social Media Security Important?

Social media platforms help us connect with friends, family, and communities. However, they are also common targets for hackers, scammers, and fake accounts. A compromised social media account can lead to identity theft, financial scams, and privacy violations.

Enable Two-Factor Authentication (2FA)

Two-Factor Authentication (2FA) adds an extra layer of security. Even if someone knows your password, they still need a second verification step to access your account. Enable 2FA for all important social media accounts.

Think Before You Share

Everything you post online creates a digital footprint. Avoid sharing your home address, phone number, live location, or travel plans before returning home. Oversharing makes it easier for scammers to target you.

Beware of Fake Giveaways

Scammers often advertise fake giveaways with messages like "Congratulations! You won an iPhone." They usually ask you to enter personal details or pay a small processing fee. Always verify giveaways through the official account of the company.

Review Your Privacy Settings

Most social media platforms allow you to control who can view your profile, see your posts, send you messages, and tag you in photos. Review these settings regularly.



Never Share Verification Codes

Social media platforms may send verification codes when someone tries to log in. Never share these codes with anyone. If someone asks for your code, they are trying to hack your account.

DEEPAKWEBCRAFTS

Chapter 6

Scam Awareness

What Is an Online Scam?

An online scam is a dishonest attempt to trick people into giving away their money, personal information, passwords, or banking details. Scammers often pretend to be trusted organizations. Their goal is to create panic, excitement, or urgency.

1. OTP Scam

An OTP (One-Time Password) is meant to verify your identity. No genuine bank, payment app, or company will ask you to share your OTP over a phone call, message, or email.



The Golden Rule of UPI

Receiving money never requires entering your UPI PIN. You only enter your UPI PIN when you are SENDING money.

2. UPI and QR Code Scams

Scammers send a "Collect Request" on UPI apps. If you approve it, money leaves your account. Similarly, scanning a QR code can lead to a payment request. Always read the confirmation screen before approving anything.

3. Fake Customer Support Scam

Scammers create fake customer care numbers online. When victims call them, the scammers may ask them to install a remote access app, share banking details, or make unnecessary payments. Always obtain customer support numbers from official websites.

4. Job & Lottery Scams

Fake job offers promise high salaries but ask for "registration fees". Legitimate employers generally do not ask applicants to pay money simply to apply. Similarly, if you receive a message saying you won a lottery you didn't enter, it is a scam.

5. Social Engineering

Social engineering is the art of manipulating people instead of hacking computers. Scammers convince victims to reveal sensitive information willingly by pretending to be police officers, courier executives, or bank employees.

Scam Safety Checklist

- ☐ Never share OTPs.
- ☐ Never share your UPI PIN.
- ☐ Verify unknown callers.
- ☐ Ignore unexpected prize messages.
- ☐ Read payment confirmation screens carefully.
- ☐ Stay calm—scammers rely on panic and urgency.

Chapter 7

Banking & Payment Safety

Protect Your Banking Credentials

Your banking credentials include your Login ID, Password, Debit/Credit Card Number, ATM PIN, CVV, UPI PIN, and OTP. These details should always remain private. Never share them with anyone, even if the caller claims to be from your bank.

Understand the Difference

OTP: Verifies identity. Valid for a short period. Never share.

ATM PIN: Authorizes ATM and debit card transactions. Keep confidential.

UPI PIN: Used ONLY when sending money via UPI. Never share.

Use Official Banking Apps

Download banking applications only from Google Play Store or Apple App Store. Avoid downloading modified banking apps from websites or unknown links.

Check Transaction Alerts

Enable SMS and email notifications for your bank account. These alerts help you detect unauthorized transactions quickly. If you receive an alert for something you did not do, contact your bank immediately.

Avoid Banking on Public Wi-Fi

Public Wi-Fi networks may not be secure. Avoid using them for internet banking, UPI payments, or viewing account statements.

Be Careful with Debit and Credit Cards

When using your card, do not let it out of your sight. Cover the keypad while entering your PIN. Report a lost or stolen card immediately through your bank's official app or customer support.

DEEPAKWEBCRAFTS

Chapter 8

What to Do If You Get Hacked

Stay Calm

Discovering that one of your accounts has been hacked can be stressful. However, panicking often leads to poor decisions. Take a deep breath and act quickly, but carefully.

Signs That Your Account May Be Hacked

- You cannot log in with your password.
- You receive login alerts from unknown devices.
- Messages are sent from your account without your knowledge.
- Your password or email address has been changed.
- You notice unauthorized transactions.



Step 1: Change Your Password Immediately

If you still have access to your account, change your password immediately. Create a new, strong, unique password. Do not reuse an old password.

Step 2: Enable Two-Factor Authentication (2FA)

After changing your password, enable 2FA. This adds an extra layer of security and helps prevent unauthorized access.

Step 3: Review Account & Log Out Everywhere

Review your account settings and confirm that your recovery email and phone number are correct. Most platforms allow you to view devices that are currently signed in. Log out any unfamiliar devices.

If Your Gmail Is Hacked

Because many other accounts are connected to your email, securing it should be your top priority. Use Google's official account recovery process immediately.



Learn From the Incident

Ask yourself: Did I reuse a password? Did I click a suspicious link?

Understanding what happened can help prevent similar incidents in the future.

Chapter 9

Daily Cyber Habits

Why Good Habits Matter

Cybersecurity is not something you do once. It is a daily habit. Most cyber attacks succeed because people make small mistakes—not because hackers are extremely skilled.

✓ Daily Cyber Checklist

- ☐ Lock your device when not in use.
- ☐ Keep software updated.
- ☐ Think before you click on suspicious links.
- ☐ Verify payment requests.
- ☐ Monitor important notifications.
- ☐ Use trusted internet connections.

Weekly & Monthly Cyber Habits

Weekly: Review installed apps, verify privacy settings on social media, and back up important photos and documents.

Monthly: Update recovery phone numbers, check active devices signed into your accounts, and review banking statements.

The 10 Golden Rules of Cyber Safety

1. Never share your OTP.
2. Never share your UPI PIN.
3. Use strong, unique passwords.
4. Enable Two-Factor Authentication.
5. Download apps only from official stores.
6. Keep your devices updated.
7. Verify links before clicking.
8. Avoid oversharing personal information online.
9. Be cautious of urgent or unbelievable offers.
10. Stay informed about new online scams.

Chapter 10

Cybersecurity Glossary

Cybersecurity includes many technical terms that may seem confusing. This glossary explains the most common words in simple language.

DEEPAKWEBCRAFTS

Antivirus: A program designed to detect, block, and remove harmful software from your device.

Browser: The application you use to access websites (e.g., Chrome, Edge, Safari).

Cookie: A small file that websites save on your device to remember your preferences or track activity.

Encryption: Converts readable information into a coded format that can only be read by authorized users.

Firewall: A security system that monitors and controls incoming and outgoing network traffic.

Malware: Any software intentionally created to harm a device or steal information (e.g., Virus, Ransomware).

Phishing: A scam in which attackers pretend to be trusted organizations to trick people into revealing sensitive information.

Two-Factor Authentication (2FA): An additional security feature that requires a second verification step after entering your password.

VPN (Virtual Private Network): Creates a secure connection between your device and the internet, improving privacy.

Final Thoughts & Conclusion

Cybersecurity does not require you to be a computer expert. It requires awareness, careful decision-making, and good digital habits. Most online threats can be avoided by following the simple practices explained in this guide.

Technology will continue to evolve, and so will cyber threats. The best defense is to stay informed and remain cautious whenever you are online. Cybersecurity is not about fear—it's about awareness. Every strong password, every verified website, and every careful decision makes your digital life safer.

Stay Safe. Stay Smart. Stay Secure.

DEEPAKWEBCRAFTS

© 2026 Deepak Webcrafts

All Rights Reserved.

This PDF is intended for educational and awareness purposes only.

No part of this PDF may be copied, reproduced, redistributed, resold, or transmitted in any form without prior written permission from the author, except for brief quotations used in reviews or educational references.

Unauthorized distribution may violate applicable copyright laws.

Thank You!

Thank you for reading **Cybersecurity for Everyone**.

I hope this guide helps you stay safer online and protect your digital life.

Contact / Support

 **Email:** deepaksonihr0021@gmail.com

 **Instagram:** [@deepaksonihr21](https://www.instagram.com/deepaksonihr21)

Stay Safe.
Stay Smart.
Stay Secure.