
Cyber Security
Simple Steps to Protect Your Digital World

# What is Cyber Security?

## Digital Locks for Digital Homes

Think of your computer and accounts like your house. You wouldn't leave your front door wide open, right?

**Cyber security** is simply the practice of locking your digital doors. It protects your personal information, your money, and your privacy from thieves who want to steal them online.

# The 3 Pillars of Safety

## Confidentiality

Only the right people can see your stuff. Like a sealed letter, not a postcard.

## Integrity

Nobody can change your data without you knowing. Your files stay exactly how you left them.

## Availability

Your information is there when you need it. No crashes, no lockouts.

# The "Bad Guys"

## Malware

Short for "Malicious Software." It's like a flu for your computer that makes it sick, slow, or steals info.

## Ransomware

A digital kidnapping. Hackers lock your files and demand money (a ransom) to unlock them. **Never pay the ransom!**

# Don't Bite the Hook!

## What is Phishing?

Scammers send fake emails pretending to be your bank, your boss, or Netflix. They want you to panic and click a link.

## How to Spot it:

- Check the sender's email address carefully.
- Hover over links before clicking.
- Watch out for bad spelling or "Urgent Action Required!" threats.

# Building a Fortress

## The Don'ts

- Don't use "123456" or "password".
- Don't use your dog's name or birthday.
- Don't use the same password for every website.
- Don't write it on a sticky note attached to your monitor!

## The Do's

- Use at least 12 characters.
- Mix letters, numbers, and symbols.
- **Use a Passphrase:** "Purple-Elephant-Pizza-99!" is strong and easy to remember.
- Use a Password Manager to remember them for you.

# Double the Lock

## Multi-Factor Authentication (MFA)

This is the single best thing you can do for security.

It adds a second step to logging in. Even if a hacker steals your password (the key), they can't get in because they don't have your phone (the second lock).

**Always turn on 2FA/MFA when available.**

# Close the "Open Windows"

## Software Updates Matter

We all hate that pop-up: "Update Ready to Install." But ignoring it is dangerous.

Hackers look for "holes" in old software to sneak in. An update is basically the company patching that hole.

**Rule of Thumb:** If it asks to update, click "Yes" immediately.

# Surfing Safely

## HTTPS

Look for the little lock icon in your browser address bar. It means your connection is secure.

## Public Wi-Fi

Avoid checking bank accounts at coffee shops. Public Wi-Fi is often not secure.

## VPN

Use a Virtual Private Network (VPN) if you must work remotely. It creates a secure tunnel for your data.

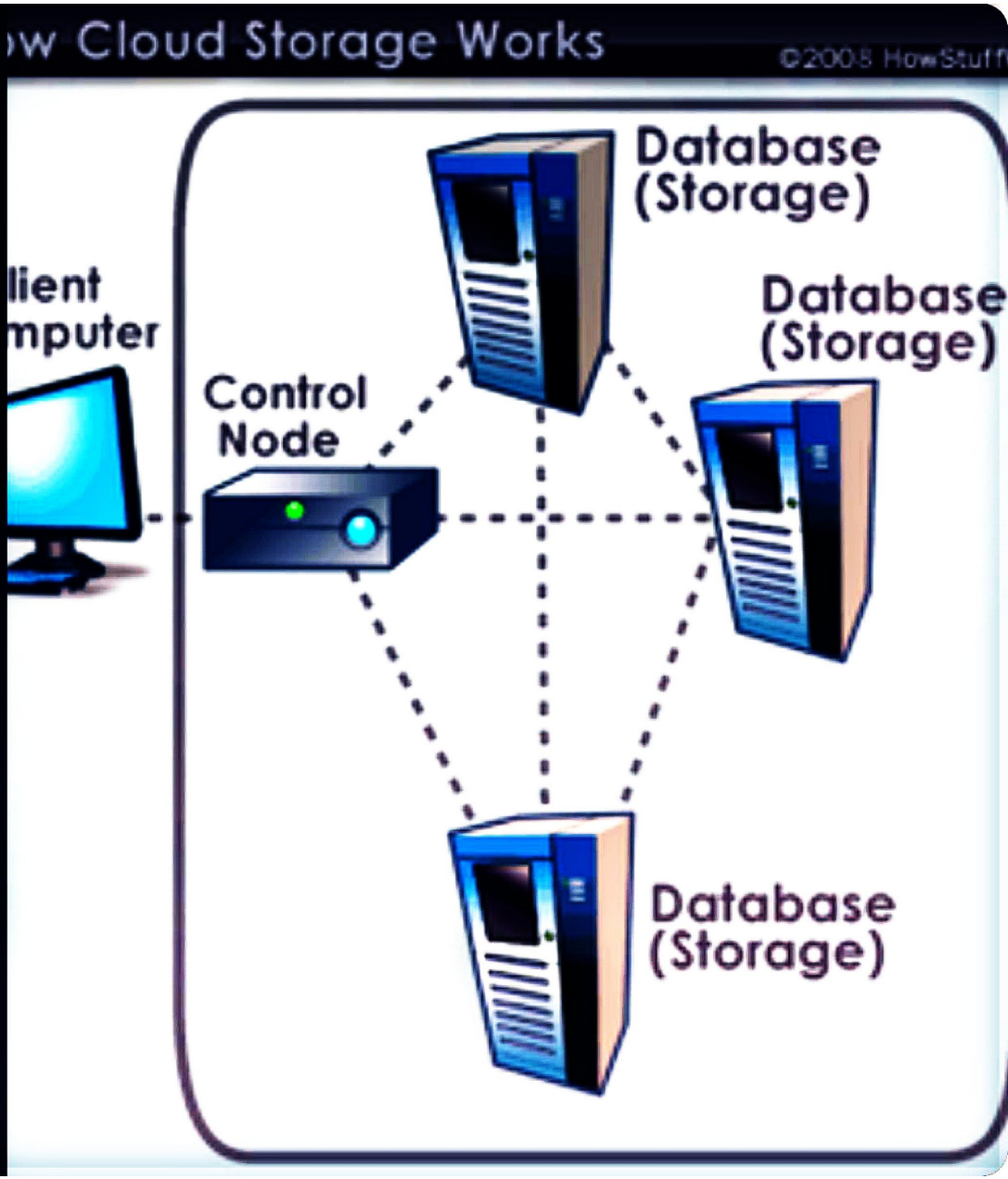
# Your Safety Net

## Back It Up!

Imagine if your laptop broke today. Would you lose everything?

**Backups** ensure that even if you get hacked or delete a file by mistake, you can get it back.

Use an external hard drive or a cloud service like Google Drive or OneDrive.



# Your Security Checklist

- **Use Strong Passwords:** Long, unique phrases are best.
- **Turn on MFA:** Protect your accounts with that extra step.
- **Think Before You Click:** Inspect emails for fishing hooks.
- **Update Everything:** Keep your digital doors patched.
- **Back Up Data:** Save your important files offline or in the cloud.


Thank You!
Security is everyone's responsibility.
security@yourcompany.com