

# Top 5 Mistakes That Lead to Hacks

- In today's digital world, cyber threats are more common than ever. Many people fall victim to hackers not because of advanced attacks, but because of simple, avoidable mistakes. Here are the top five mistakes that often lead to hacks—and how to protect yourself from them.

## 1. Using Weak or Reused Passwords

One of the most common security mistakes is using weak or reused passwords. Many people still rely on simple passwords like “123456” or reuse the same password across multiple accounts. If a hacker gains access to one account, they can often access others easily.

**Tip: Use strong, unique passwords that include a mix of letters, numbers, and symbols. Consider using a password manager to keep track of them securely.**

## 2. Clicking Unknown Email Links (Phishing)

Phishing emails trick users into revealing personal information by pretending to be from trusted companies. A single careless click can give hackers access to your bank details or login credentials.

**Tip: Always verify the sender's address before clicking any link. Hover over links to see the real URL and never download attachments from unknown sources.**

## 3. Ignoring Software Updates

Delaying software updates might seem harmless, but it leaves your device exposed to known security flaws. Hackers often exploit outdated systems to gain access.

**Tip: Turn on automatic updates for your operating system, antivirus, and applications. Regular updates close security loopholes and protect you from newly discovered threats.**

## 4. Sharing Personal Information on Social Media

Oversharing on social platforms can give hackers the details they need to impersonate you or answer security questions. Even simple information like your pet's name or birthday can be used in password guessing.

**Tip: Limit what you share publicly. Review your privacy settings regularly and avoid posting sensitive details such as your location or personal documents.**

## **5. Using Unsecured Public Wi-Fi Without a VPN**

Public Wi-Fi networks, such as those in cafes or airports, are often unsecured. Hackers can intercept data transmitted over these networks, including your passwords and personal information.

**Tip: Avoid accessing sensitive accounts on public Wi-Fi. If necessary, use a reliable Virtual Private Network (VPN) to encrypt your connection.**

### **Final Thoughts**

**Most cyberattacks can be prevented with a bit of awareness and caution. By creating strong passwords, staying alert to phishing attempts, keeping your software up to date, protecting your privacy on social media, and using secure networks, you can greatly reduce your risk of being hacked. Cybersecurity starts with smart everyday habits.**