Cybersecurity: Stay Safe Online!

Cybersecurity is the protection of computers, phones, and the internet. It helps keep personal information safe. Hackers are people who try to steal passwords, bank details, or private data. Many hackers use **dishonest** tricks, like sending **misleading** emails that look real but are fake. If people **misplace** their passwords, they may **lose** access to their accounts. Some hackers use **illegal** programs to **unlock** private data.

To stay safe, always use a strong password. A strong password has numbers, symbols, and both big and small letters. It is also good to **reset** your password often. If you **overuse** the same password everywhere, hackers can guess it easily. Many users **disregard** security rules, making their accounts **unsafe**.

One great way to protect accounts is **two-factor authentication (2FA)**. This means that after entering a password, a person also needs a code from their phone or email. This extra step makes hacking difficult. Many websites now **overprotect** accounts by asking for 2FA every time you log in. If you **disable** this feature, your account becomes **vulnerable** to attacks.

Another danger is **phishing**. This happens when someone sends a fake email or message asking for passwords. These emails look real, but they are tricks. Never click on strange links or give personal information in emails. If an email has **nonsense** words, asks for money, or comes from an **unknown** sender, it is probably fake. **Mistaking** a phishing email for a real one can be dangerous.

Some hackers use the **dark web**, a **sublevel** of the internet where they sell stolen information. Many businesses use **nonstop** security checks to make sure their data is safe. Companies that **undervalue** cybersecurity often suffer serious losses. A **substandard** security system can put important information at risk.

To fight cyber threats, companies install **antivirus** software. This helps detect and remove dangerous programs. Some businesses also create **prevention** plans to stop attacks before they happen. Others use **firewalls** to **block** attacks and **recover** lost data. Without these **protective** measures, hackers can **disable** entire systems.

Without **proper** cybersecurity, people and businesses are in danger. But if we follow simple steps, like updating passwords, using **secure** connections, and not opening strange emails, we can **reduce** the risk and stay safe. Experts often **review** security systems to make sure they remain effective.

Questions

1.What is cybersecurity?
A) A way to protect computers and the internet
B) A way to fix broken computers
C) A type of computer game
D) A way to make websites faster

2.What does the word dishonest **mean?**
A) Telling the truth
B) Not honest
C) Very smart
D) A type of hacker

3.What does reset **mean?**
A) To use again
B) To set again or change
C) To stop working
D) To write a password

4.**What is phishing?**
A) A fake email that tries to steal passwords
B) A type of online shop
C) A strong password system
D) A tool to fix computers

5.What does prevention **mean in the text?**
A) Something that happens after an attack
B) Stopping something before it happens
C) A way to create a strong password
D) A tool for fixing computers

6.What does antivirus **software do?**
A) Protects computers from viruses
B) Deletes all passwords
C) Makes computers faster
D) Creates websites

7.What does **recover** mean in the text?
A) To get something back
B) To lose data
C) To stop working
D) To create a new password