



Computer Security

Cybersecurity Awareness

Protecting Your Computer

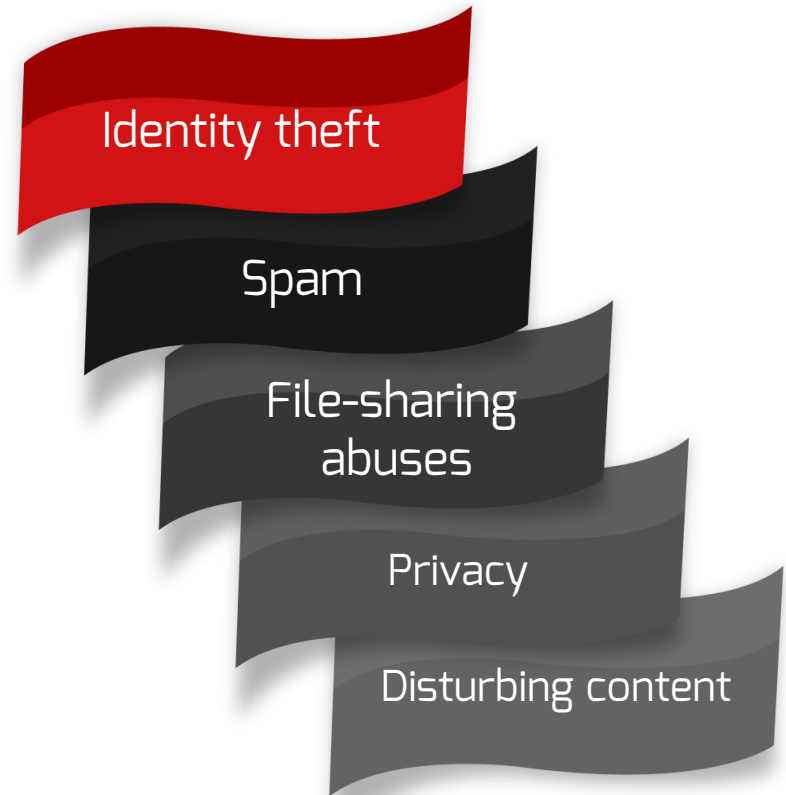
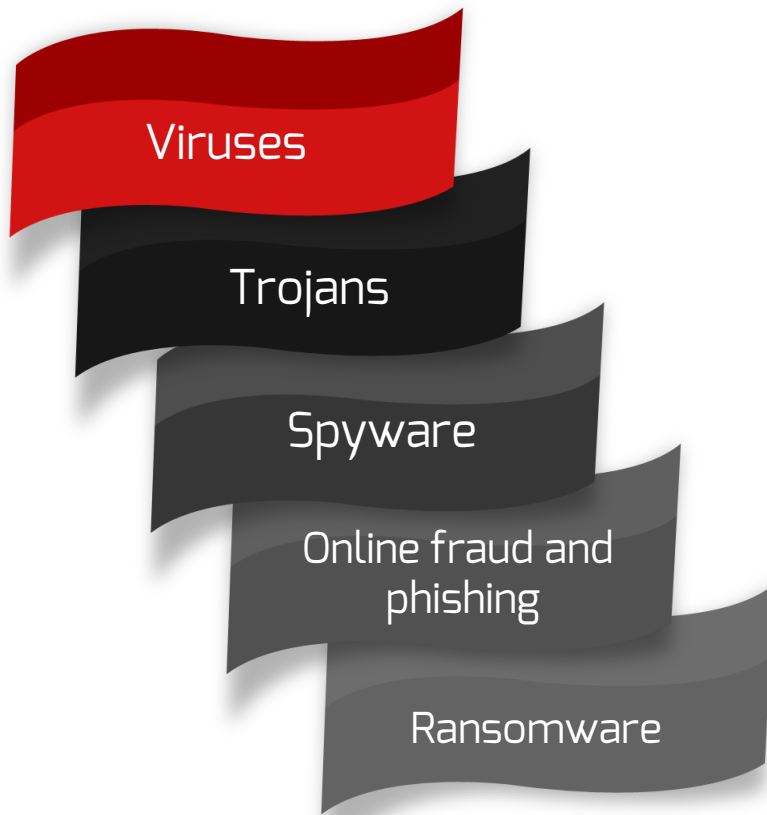




Risks

Risks

Risks associated with computers



Risks

Virus

Virus is a program designed specifically to damage or copy data from your computer.

01

Trojans

Trojan is a program that apparently seems legitimate but is actually a malicious program that damages data in a computer and steals sensitive information.

02

Spyware

A program that spies on your computer and tracks your activities.

03

Online fraud and phishing

Attackers usually send email to users and compel them to reveal personal information or make online transactions.

04

Ransomware

A type of malware which encrypts user data and demands an amount of money to be paid to provide the user with the decryption key.

Identity theft

Criminals gain access to your personal information and use it to steal money, make transactions or perform other similar activities.

Spam

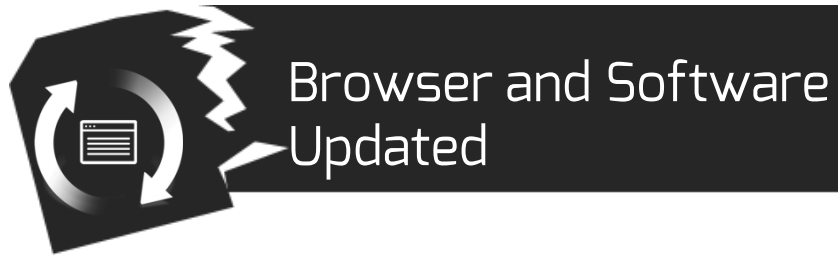
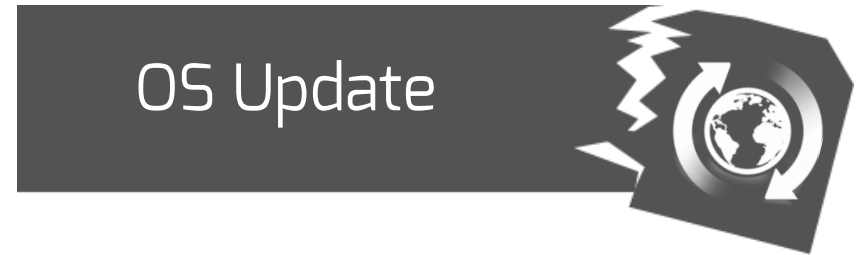
Spam are emails which you have not subscribed, but still receive it.



How to Protect your Computer?

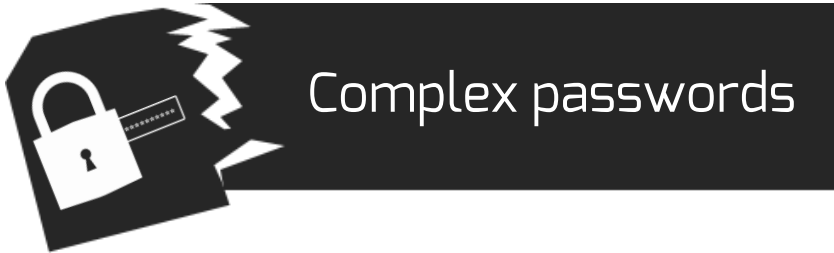
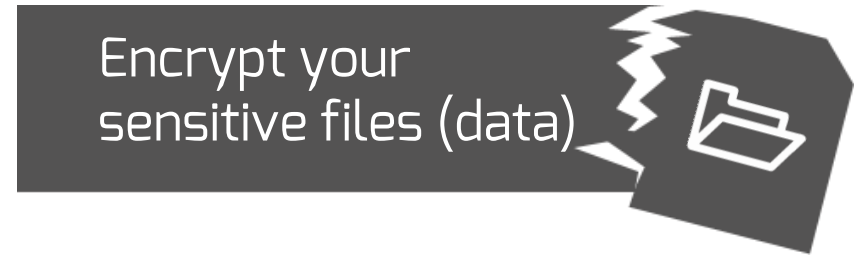
How to Protect from Computer Threats?

You can protect your computer by using following techniques:

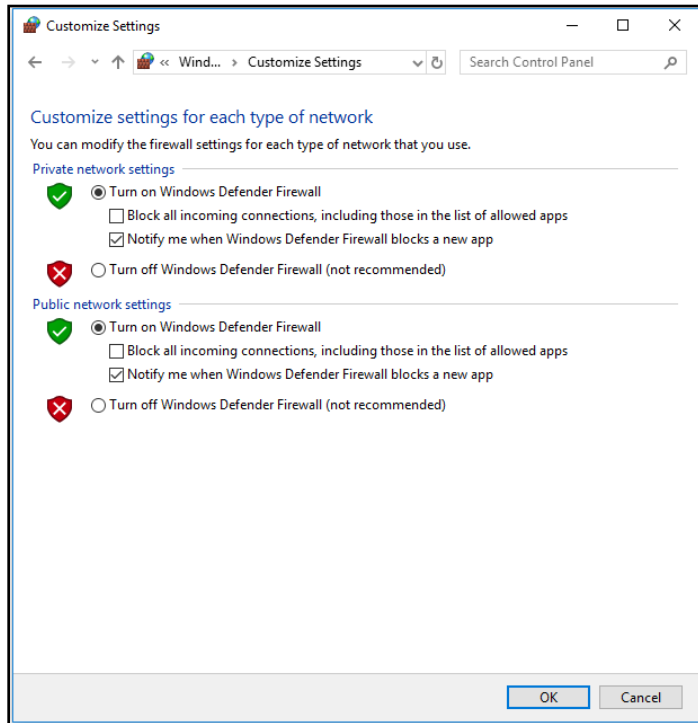


How to Protect from Computer Threats?

You can protect your computer by using following techniques:



Desktop Firewall



Stops unauthorized inbound connections.

Can also filter outbound connections.

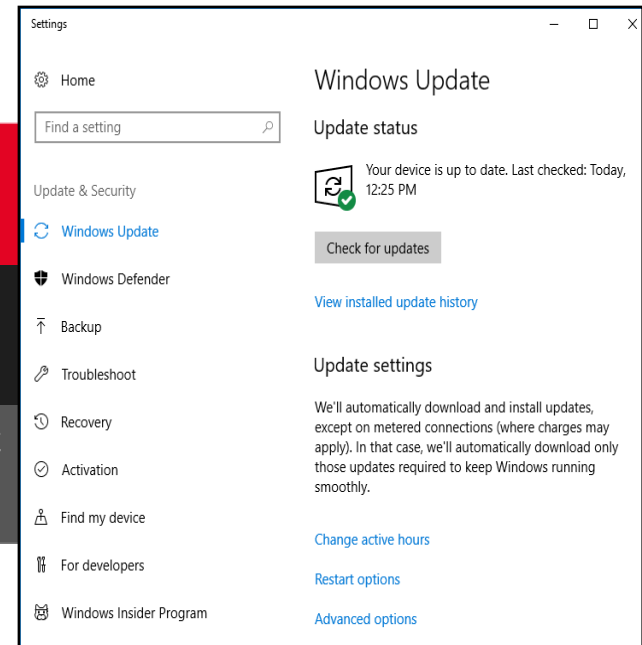
Should keep Desktop Firewall activated.

Operating System Update

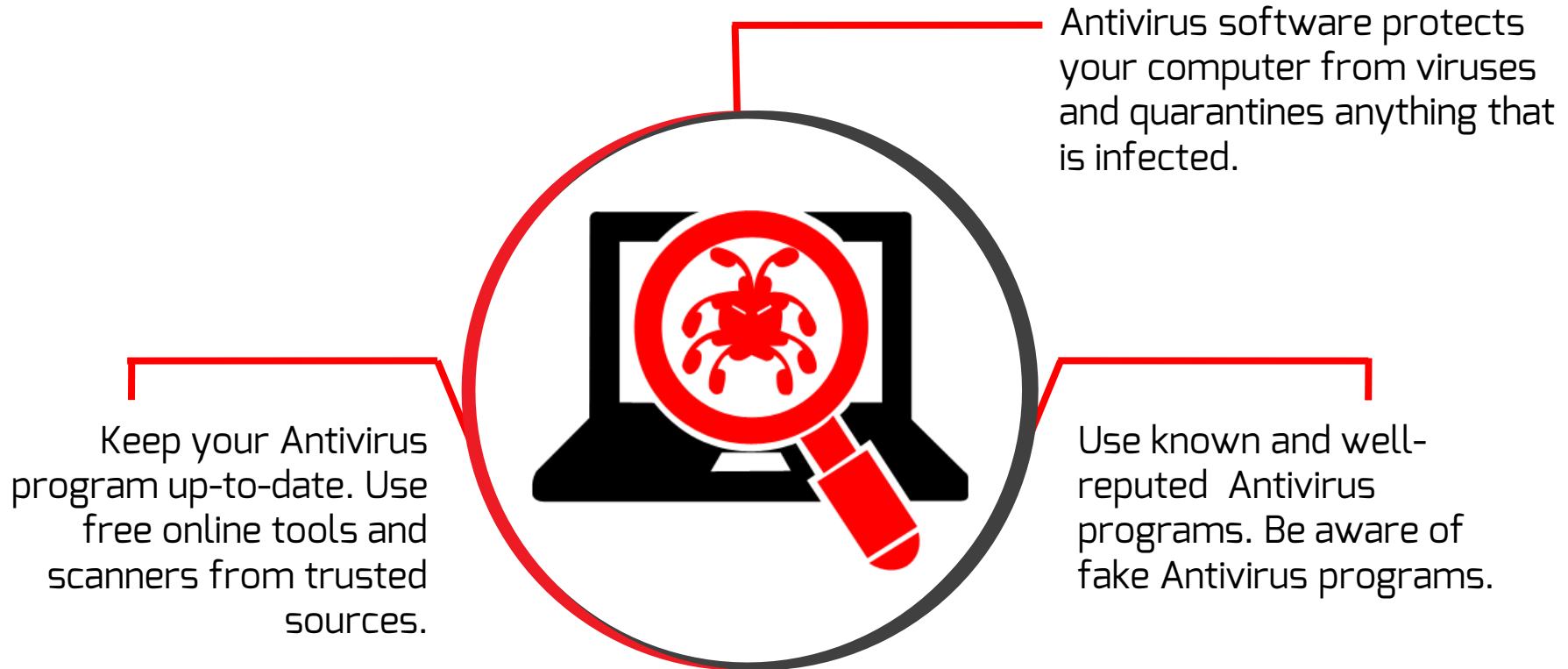
Updates / patches known vulnerabilities.

Users are required to restart their machines to complete the patch installation.

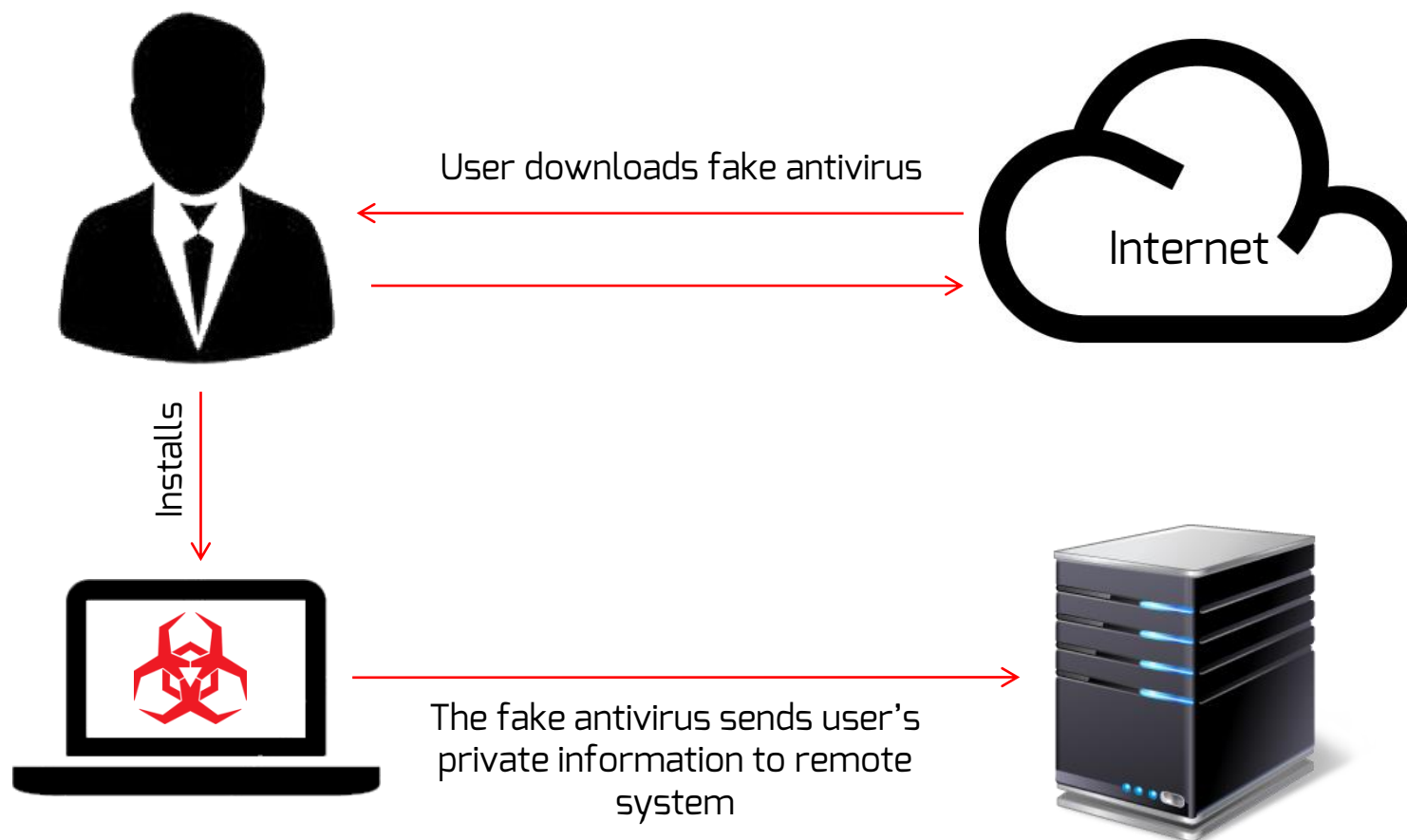
Should keep OS update settings to automatic download and manual installation.



Antivirus



Be careful from: Fake Antivirus



Browser Update



01

While using internet, there is a high probability that you end up using a malicious website or download a software that has virus attached with it.

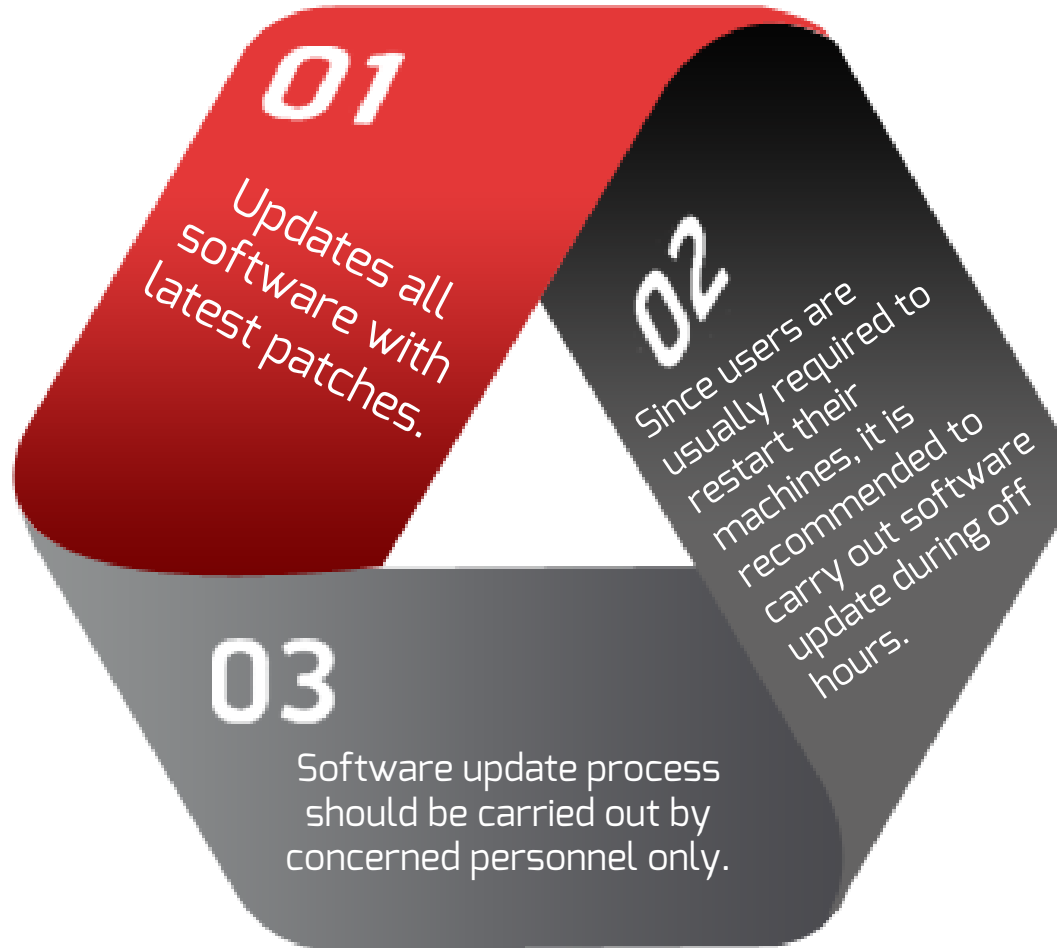
02

Updating browser provides you one way of using internet securely.

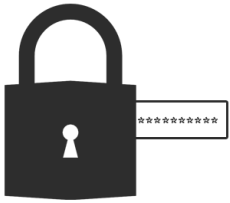
03

The patch provides better security against viruses, trojans, phishing and other threats.

Software Update



Complex Passwords



01

You should use complex passwords which are easy to remember but hard to guess.



03

Frequently change passwords.



05

Username should not be used as part of password.



02

Use passwords that contain minimum of 8 characters.



04

Every password should contain alphanumeric and special characters.

Application Download

01



Downloading applications from internet is one of the biggest threats as the user may be tricked to download application from a source that seems legitimate but actually contains virus/malware with it.

02



Always download application **from legitimate source** e.g. if you have to download a smartphone application, download it from its official store (App Store, Google Play, etc.).

Encryption



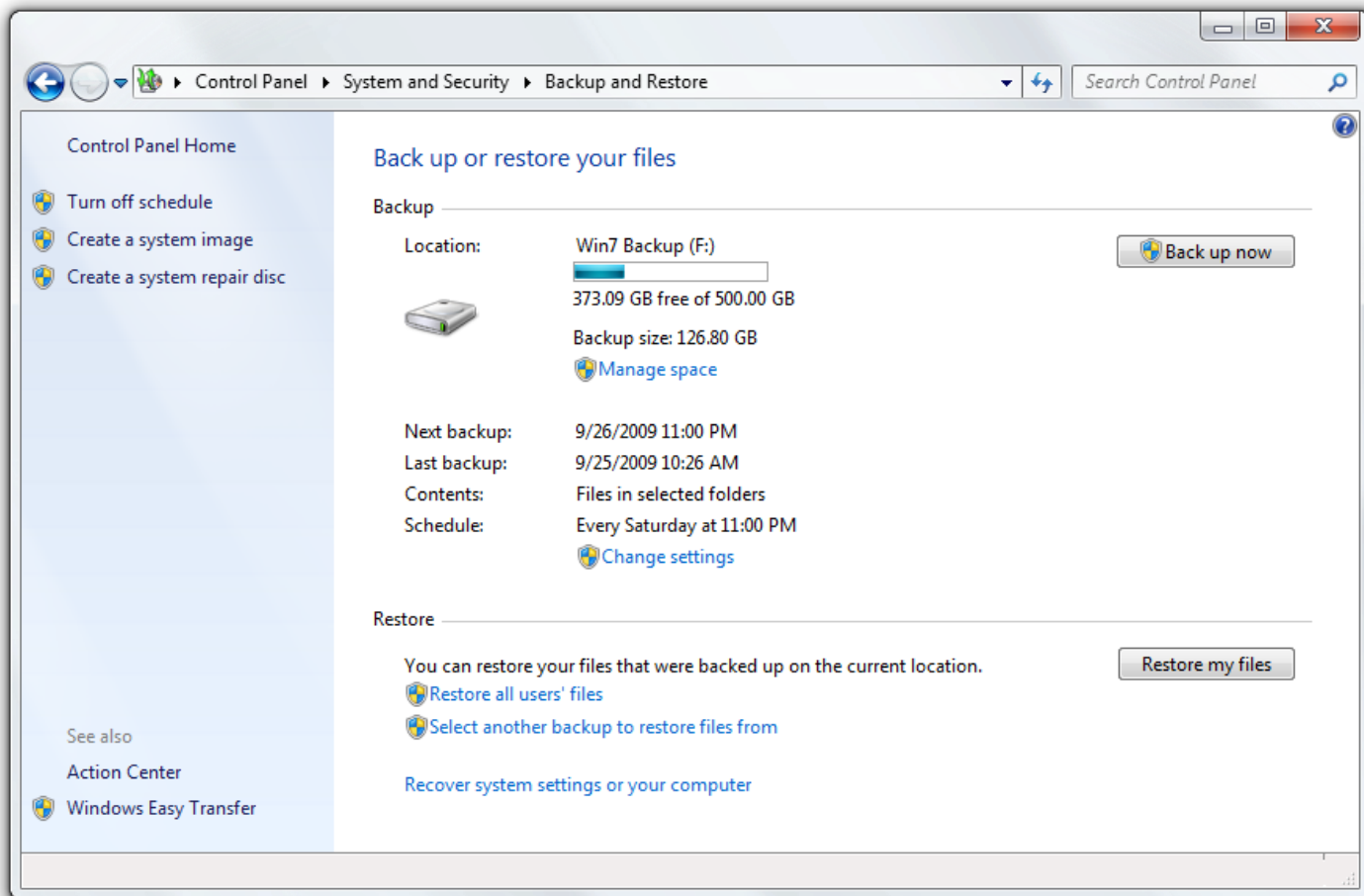
Backup and Recovery

Backup is an extra copy of your data.

Backup is used when data is corrupted or lost.

The backup strategy defines how often and when the data will be backed up.

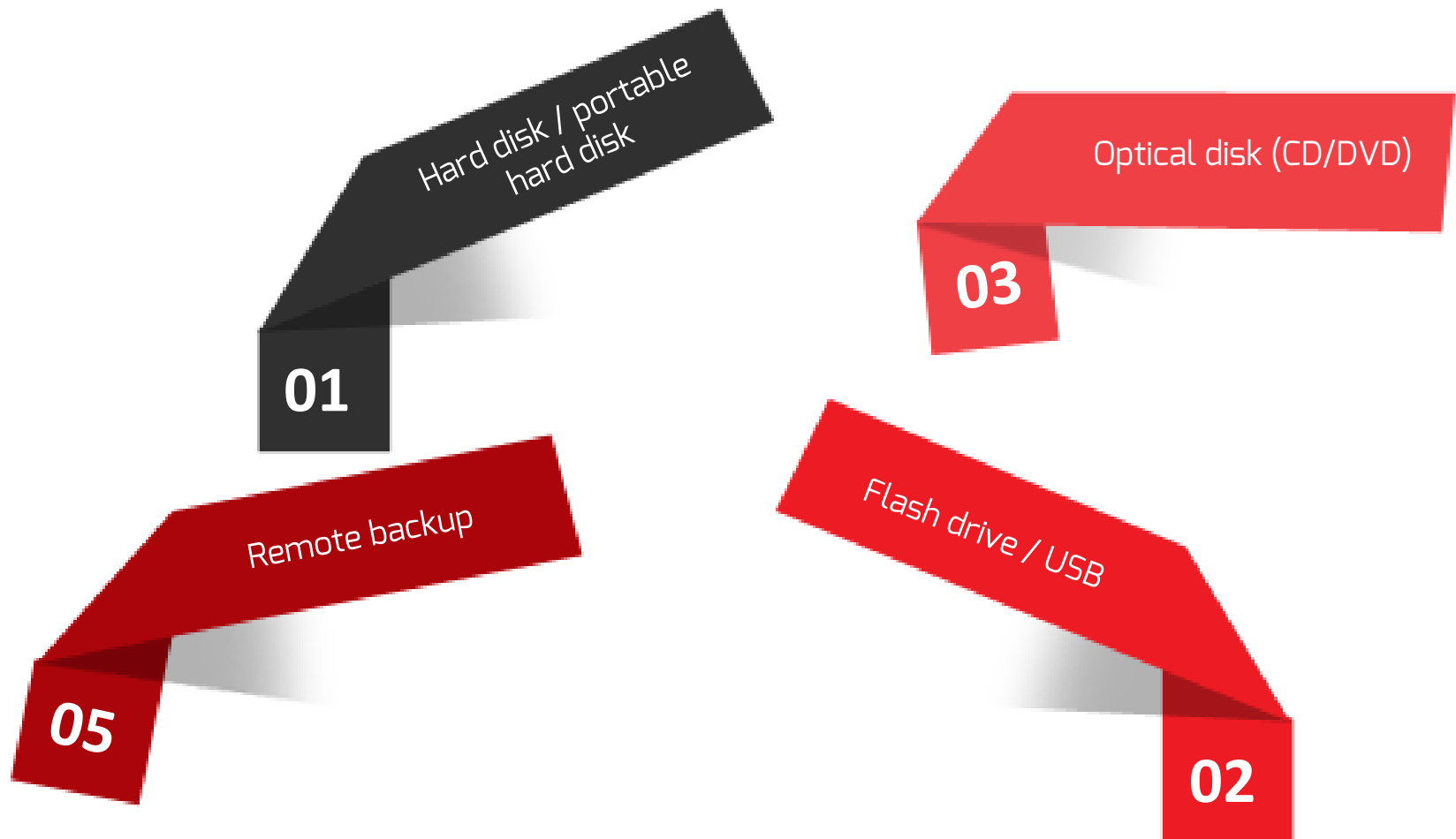
Backup and Recovery - Windows



Backup and Recovery - Mac



Backup Media





Best Practices

Best Practices



Turn On Desktop Firewall




Update Your OS



Encrypt your Data



Update Your Applications



Backup You Data



Update Your Browser



Use Updated Antivirus

Questions

WHAT? HOW? WHEN?
WHO? WHERE? WHO?
WHEN? WHY? WHAT?
HOW? WHO?
WHAT? WHERE?
WHO? WHERE?
WHAT? WHO?
HOW? WHERE?
WHY? WHAT?
WHERE? WHEN?
WHAT? WHERE?
HOW? WHO?
WHO? WHERE?
WHY? WHAT? HOW?
HOW? WHEN? WHERE?
WHAT? WHEN? WHERE?
WHO? WHY? HOW?
HOW? WHERE?
WHAT? WHY?
WHEN? WHO?
WHO? WHAT?
WHERE? WHAT? HOW?
WHO? WHY? WHERE?
WHAT? WHEN?

WHERE?
WHO? WHAT?
WHERE? WHY?
HOW? WHEN?
WHAT? WHO?
WHY? WHERE?
WHEN? HOW?
HOW? WHERE? WHO? WHAT?
WHY? WHAT? WHEN?
WHERE? HOW?
WHEN? WHO?
WHERE?