

Name _____

WORKSHEET 15 – INFORMATION SECURITY

Make sure that you are familiar with all of the information detailed in this booklet. There are a number of tasks for you to carry out, be sure to read the information fully whilst completing the tasks. You could be asked about any of this in the test!

Use the theory notes in the worksheet 15 section of the teach-ict.com site to help you complete this booklet.

TASK 1: COMPUTERS VS DATA

Which is the most valuable, a computer or the data it contains? Explain your answer.

THE DATA IS THE MOST VALUABLE. YOU COULD GO OUT TODAY AND BUY A NEW COMPUTER IF YOURS WAS STOLEN OR BROKE DOWN. BUT IT WOULD TAKE YOU A LONG TIME TO REPLACE THE DATA – AND IT MIGHT NOT EVEN BE POSSIBLE.

TASK 2: IMPLICATIONS OF DATA LOSS

If a company were to lose all of its data, it could face a number of problems. Discuss three possible problems below.

- CONFIDENTIAL DATA ABOUT CUSTOMERS SUCH AS NAMES, ADDRESSES, CREDIT CARD DETAILS MIGHT FALL INTO THE WRONG HANDS
- CONFIDENTIAL DATA ABOUT STAFF MIGHT FALL INTO THE WRONG HANDS
- A COMPETITOR MIGHT GET HOLD OF ALL OF THE RESEARCH OR PRODUCT DEVELOPMENT IDEAS OR CUSTOMER LISTS
- CRIMINALS MIGHT GET HOLD OF YOUR BANK DETAILS AND TRY TO STEAL MONEY
- A CRIMINAL COULD TRY TO BLACKMAIL THE COMPANY

ACCEPT ANY SENSIBLE ANSWER

TASK 3: USER NAMES AND PASSWORDS

Explain why you need both a user name and a password in order to log into a network.

A USER NAME IDENTIFIES YOU TO THE NETWORK AS SOMEONE WHO IS ENTITLED TO LOG ON.

A USER NAME HAS YOUR ACCESS RIGHTS ASSIGNED TO IT

YOU ALSO NEED A PASSWORD TO PROVE THAT THE USER NAME REALLY BELONGS TO YOU

List 4 sensible rules for keeping a password safe.

- DON'T TELL ANYONE ELSE YOUR PASSWORD
- DON'T WRITE YOUR PASSWORD DOWN
- DON'T PICK A PASSWORD THAT WOULD BE EASY TO GUESS
- CHANGE YOUR PASSWORD REGULARLY
- USE A MIX OF LETTERS, NUMBERS AND SYMBOLS

TASK 4: ACCESS RIGHTS

Using the words in the table below (just once each), fill in the blanks in the text.

LEVELS	MANAGER	ALTER	DEPARTMENTS
DETERMINE	LOWEST	HIGHEST	DELETE
NETWORK	NEW	SECURITY	READ

Every person who uses a computer **NETWORK** will be assigned a level of access rights.

Their access rights will **DETERMINE** what they are able and not able to do on the network.

Those with the **HIGHEST** level of access rights, for example the network **MANAGER**, would be able to install and **DELETE** software. They would also be able to set up **NEW** users and assign their access rights to them.

Those with the **LOWEST** level of access rights might only be able to **READ** data in files but not **ALTER** anything. Access rights helps to maintain the **SECURITY** of the system and the safety of the data held on it.

There may be many **LEVELS** of access rights within an organisation, especially as different **DEPARTMENTS** need access to different systems or parts of a system.

TASK 5: VIRUSES

Using the words in the table below (just once each), fill in the blanks in the text.

In your own words, explain what a computer virus is

A COMPUTER VIRUS IS A PIECE OF SOFTWARE CODE OR A PROGRAM WHICH IS DESIGNED TO COPY ITSELF AND CAUSE DAMAGE TO DATA OR ATTACH ITSELF TO OTHER PROGRAMS

Can viruses cause a lot of damage to a computer? Yes / No

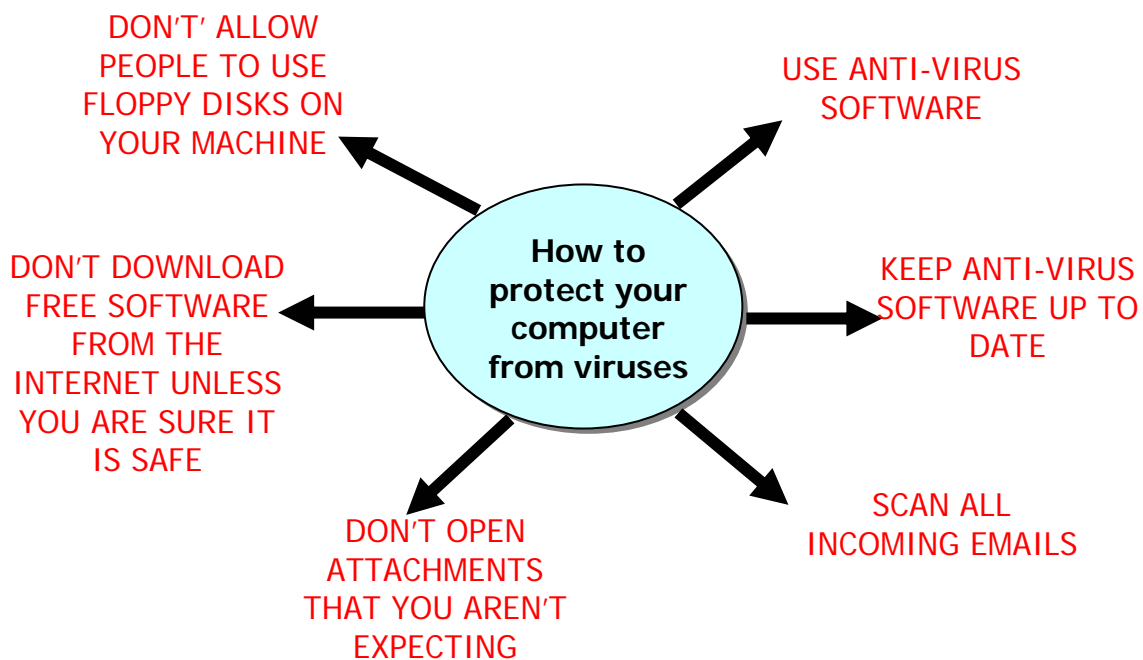
Explain your answer

A VIRUS DOES NOT DAMAGE THE HARDWARE, IT ATTACKS THE SOFTWARE AND DATA

Computer Viruses can be spread by:

- OPENING ATTACHMENTS IN EMAILS
- FILES STORED ON REMOVABLE MEDIA E.G. FLOPPY DISKS
- DOWNLOADING FREE SOFTWARE FROM THE INTERNET
- CLICKING ON SOME POP-UPS ON WEB PAGES

Complete the diagram below to show how to protect your computer from viruses:

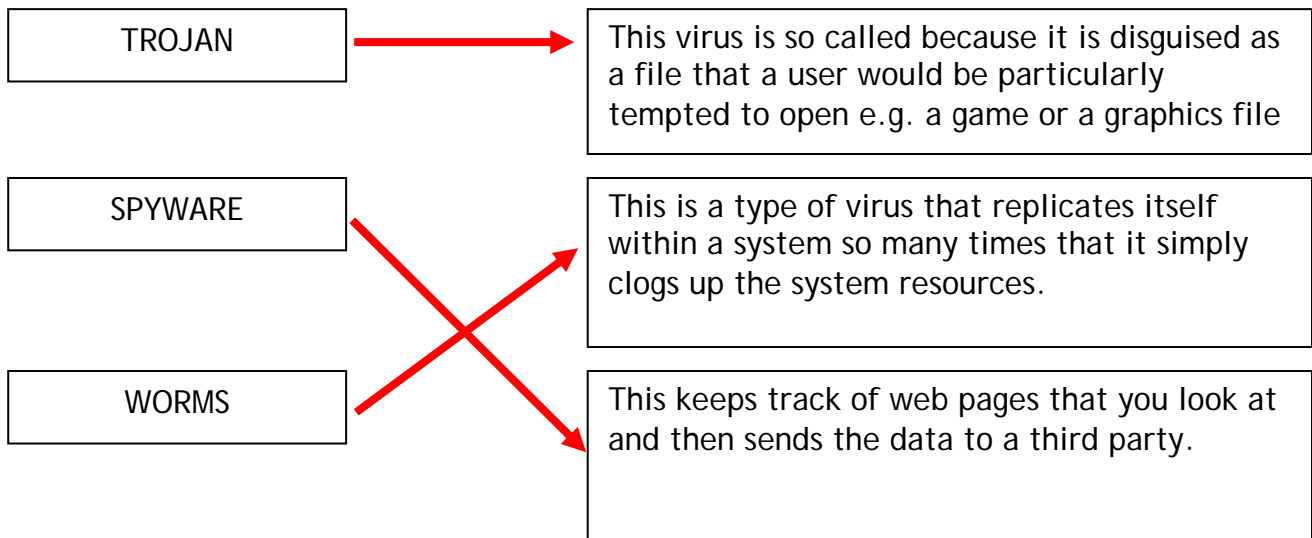


OR ANY OTHER SENSIBLE ANSWER

Why do you think it is important to keep anti-virus software up-to-date? (try to find this answer out for yourself)

BECAUSE NEW VIRUSES ARE BEING RELEASED ALL OF THE TIME AND YOU NEED TO GET THE LATEST PATCHES SO THAT YOUR ANTI-VIRUS SOFTWARE CAN DETECT AND DEAL WITH ANY NEW VIRUS

Match up the pests on the left hand side with their description on the right side.



TASK 6: HACKERS

Why might a hacker want to break into a computer system?

- FOR FUN
- FOR A CHALLENGE
- TO STEAL DATA
- TO DAMAGE DATA
- TO GET REVENGE ON AN EX EMPLOYER

ACCEPT ANY SENSIBLE ANSWER

TASK 7: FIREWALLS

Explain the role of a firewall

A FIREWALL RESTRICTS ACCESS TO YOUR NETWORK SO THAT ONLY TRUSTED USERS CAN GET IN I.E. IT STOPS HACKERS. IT CAN ALSO RESTRICT WHAT PEOPLE ARE ALLOWED TO VIEW ON THE INTERNET BY BLOCKING SITES.

TASK 8: AUDIT LOG

Explain why a company should keep an audit log

IF ANY FILES ARE DAMAGED OR DELETED, THE COMPANY CAN USE THE AUDIT LOG TO TRACE WHO WAS RESPONSIBLE. THEY CAN ALSO USE IT TO TRACK IF EMPLOYEES ARE DOING THINGS THEY SHOULDN'T E.G. SPENDING ALL DAY ON THE INTERNET INSTEAD OF WORKING

TASK 9: POLICIES AND PROCEDURES

All staff should be given training and guidelines about how to use the computer system properly and to ensure that data is kept safe.

List some rules that staff should follow:

- USE A SCREEN SAVER WITH A PASSWORD
- LOCK YOUR COMPUTER IF YOU LEAVE IT UNATTENDED
- REPORT ANY SUSPICIOUS BEHAVIOUR TO A MANAGER
- ONLY ACCESS DATA THAT YOU ARE SUPPOSED TO
- MAKE SURE THAT YOU SAVE YOUR WORK REGULARLY
- DON'T TELL ANYONE YOUR PASSWORD

ACCEPT ANY SENSIBLE ANSWER

TASK 10: SAVING WORK

Explain why you should save your work every 5-10 minutes rather than waiting until the end of the lesson

BECAUSE YOUR COMPUTER OR THE SOFTWARE COULD CRASH. IF YOU HAVE SAVED YOUR WORK REGULARLY THEN THE MOST YOU WILL LOSE WILL BE A FEW MINUTES

Explain why it is a good idea to save important work as different version numbers.

BECAUSE YOU COULD HAVE MADE AN ERROR AND NOT NOTICED IT. IF YOU KEEP SAVING OVER THE SAME FILE THEN YOU CANNOT GO BACK TO A CORRECT VERSION.

TASK 11: MAKING BACK UPS

Data stored on a network should be backed up at least once every day. Why do you think that it should be backed up so often?

BECAUSE DATA IS VALUABLE AND YOU NEED TO HAVE AN UP-TO-DATE COPY THAT CAN BE USED IF PEOPLE LOST THEIR FILES OR DOCUMENTS. EVEN LOSING A DAY'S WORK WOULD BE BAD, BUT NOT AS BAD AS A WHOLE WEEK OR MONTH.

What storage media do you think would be the most suitable for making a backup of the data on a company network? (think back to your lesson on storage devices)

MAGNETIC TAPE

Once a backup has been made of the data, where should it be stored? Explain your answer

A COPY OF THE BACKUP SHOULD BE STORED OFF SITE IN A FIREPROOF SAFE.

TASK 12: PHYSICAL SECURITY OF EQUIPMENT

List some of the physical security precautions that you could take to ensure that your computer equipment doesn't get stolen:

- LOCK THE ROOM WHEN NOT IN USE
- USE SWIPE CARDS OR KEYPADS TO ACTIVATE LOCKS
- USE SPECIAL PENS TO MARK POSTCODE ONTO EQUIPMENT
- BOLT COMPUTERS TO THE DESK
- KEEP WINDOWS SHUT AND LOCKED
- USE CCTV CAMERAS
- SECURITY GUARDS IN LARGE FIRMS

TASK 13: CHALLENGE

What was the extra fact that you found out for yourself about this topic?

END OF WORKBOOK