

CO Audio 18 : BANKING SECURITY

I. You're going to hear Jon, a bank security officer, answer some questions about his job. Before you listen, try to complete the sentences about bank security.

1. A _____ hacker is a hacker who helps organizations protect themselves against criminal hackers.
2. A _____ is a process to check to see who is connected to a network.
3. _____ fingerprinting gives information about what operating system people are using.
4. 128 bit SSL _____ encrypt data.
5. Anti-virus software can protect against viruses and _____ .
6. _____ phishing is a more targeted form of phishing.

Word bank : spear / white-hat / worms / ping sweep / TCP/IP / certificates

[TCP = *Transmission Control Protocol*]

II. These were the questions asked to Jon. Listen and match the questions 1 to 6 to Jon's answers A to E. One question was not asked, can you formulate it ?

1. What can people do to stay secure online ? _____
2. Is there anything else that people should be aware of ? _____
3. How do you go about that ? _____
4. Is it safe to use credit cards online ? _____
5. So, Jon, what sort of work do you do for the bank ? _____
6. What's the difference between you and a normal hacker ? _____
7. _____ ?

III. Read this short article about a computer infection in 2008. Try to complete the text with a partner.

Conficker has been in the news a lot recently. It is a _____¹, which, unlike a virus, does not need to be attached to an existing program to infect a machine, and which seems to receive regularly updated instructions from its controllers. It has created a _____², - a network of infected machines. Once infected, these machines are known as _____³. At this point, no one knows what the purpose of Conficker is. At present, it has infected ten million computers. These could be used for a _____⁴ attack where all the infected computers attempt to access one site simultaneously.

It is probably controlled by criminals who want to steal users'personal information, i.e _____⁵. There are a number of ways of doing this : a _____⁶ records information entered via a keyboard, _____⁷ literally harvesting users'information while they are online. We will probably soon see if Conficker consists of this type of passive monitoring _____⁸ or whether it will mount a more active attack once it receives a new set of instructions.

Word bank (III) : pharming/zombies/identity theft /botnet/keylogger/worm/spyware/denial of service

Here is the rest of his mail, fill in 1 to 6 with the sentences a to f below

a Ideally this should contain both letters and numbers.

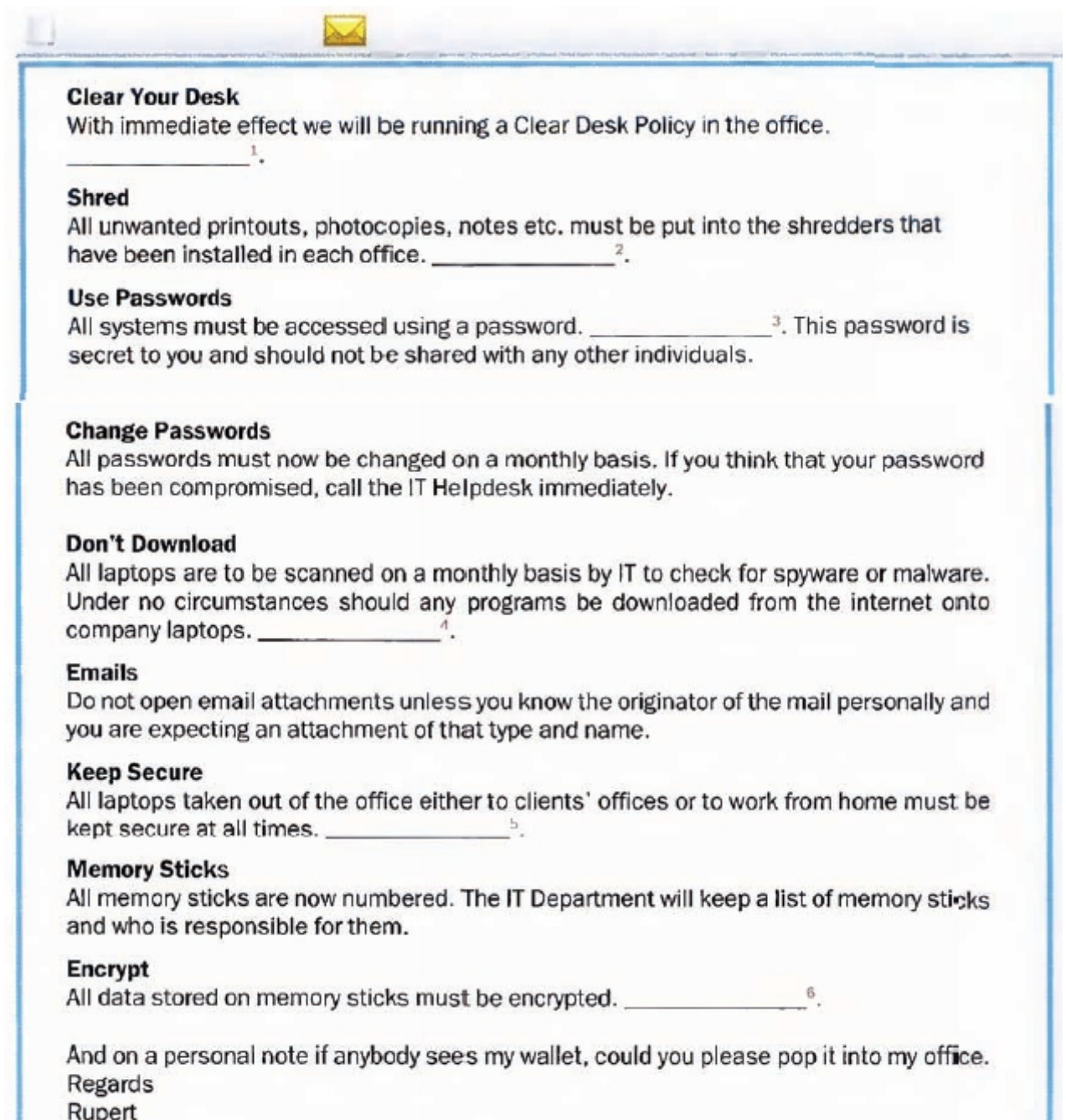
B Only company-provided and approved software may be used.

C At the end of each day, ensure that your desks are clear and all documentation or storage devices are in locked drawers.

D Do not leave them where they can be seen on the back seat of a car.

E IT will be running a webcast on how to do this next Tuesday 25th.

F Any documentation found lying around after the trading day will be destroyed. You have been warned.



Clear Your Desk
With immediate effect we will be running a Clear Desk Policy in the office.
_____ 1.

Shred
All unwanted printouts, photocopies, notes etc. must be put into the shredders that have been installed in each office. _____ 2.

Use Passwords
All systems must be accessed using a password. _____ 3. This password is secret to you and should not be shared with any other individuals.

Change Passwords
All passwords must now be changed on a monthly basis. If you think that your password has been compromised, call the IT Helpdesk immediately.

Don't Download
All laptops are to be scanned on a monthly basis by IT to check for spyware or malware. Under no circumstances should any programs be downloaded from the internet onto company laptops. _____ 4.

Emails
Do not open email attachments unless you know the originator of the mail personally and you are expecting an attachment of that type and name.

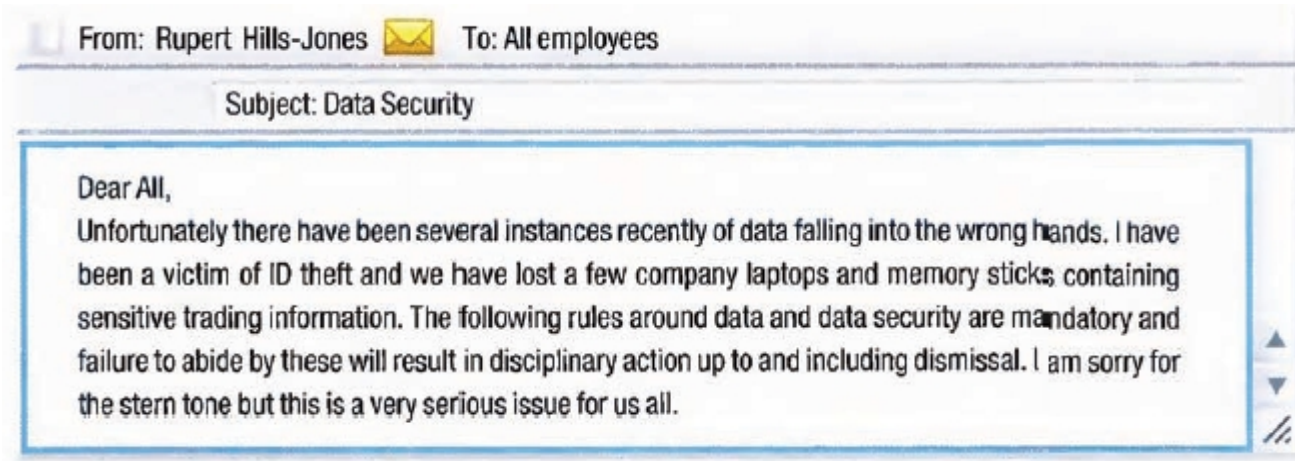
Keep Secure
All laptops taken out of the office either to clients' offices or to work from home must be kept secure at all times. _____ 5.

Memory Sticks
All memory sticks are now numbered. The IT Department will keep a list of memory sticks and who is responsible for them.

Encrypt
All data stored on memory sticks must be encrypted. _____ 6.

And on a personal note if anybody sees my wallet, could you please pop it into my office.
Regards
Rupert

At London Investments....



Recap the main information

Who is writing to whom ?

What is/are the problem(s)?

What are the consequences ?

Imagine the rules that will follow in his next mail concerning

1. printed documents

2. mails

3. passwords

4. downloading

5. memory sticks (USB keys)

6. laptops

7. ...