***Ransomware***

Hello, everyone. It’s a computer hacking trend that’s becoming increasingly widespread. It’s known as ransomware. And behind this somewhat brutish term lies a technique by which a cyber-criminal manages to block the operation of a computer, a network or a website and then demands payment of a ransom to release the system. Let’s join our reporter, Sebastian, who’s currently out and about! Sebastian, can you hear me?

Hello, Patrick. Yes, loud and clear. I’m here at business.com, a company that makes 70% of its sales via its online site. Their site has been completely locked up for 24 hours now. Hackers have encrypted the whole of their web server and demanding a ransom to release the system. Without a usable back-up business.com is not sure whether to pay, as this lock-up is costing them a significant amount of money with every hour that goes by.

Thank you, Sebastian. Joining me now is our guest, security expert Mrs. Woods. Hello, Mrs. Woods. Can you tell us what ransomware is?

Ransomware is a kind of malicious code, in the same way as viruses and Trojan horses. It’s a program which once it’s installed on your computer, spreads to the machines on your company’s network. In the vast majority of cases, it encrypts the contents of hard disks, making the stored data impossible to access. Ransomware is generally introduced via a fraudulent email that prompts its recipient either to open an attachment containing the malicious code or to click on a link that will take them to a pirate site, seeking to exploit a loophole in the browser. The ransomware also introduces text, HTML or image format files containing payment instructions. Very often, payment of the ransom takes place via websites hosted on what is known as the dark web. To avoid falling victim to ransomware, it is crucial to follow the rules given in the email awareness module. Here’s a reminder of these rules.

* Don’t click on links contained in emails that you receive
* If you need the link, copy it into the navigation bar of your browser instead
* Only open attachments that you’re expecting and that are sent by someone that you know

Thank you for your explanation, Mrs. Woods. We’ll be back shortly!