



Online safety:

Malware and phishing scams

HILLVIEW INTERNATIONAL SCHOOL – YEAR 7

Lesson Outcomes

- ▶ Be aware of the risks online, including:
 - ▶ Malware
 - ▶ Viruses
 - ▶ Trojans
 - ▶ Worms
 - ▶ Spyware
 - ▶ Adware
 - ▶ Ransomware and scareware
 - ▶ Phishing scams

Malware

- ▶ Most people mean “malware” when they say “virus”
- ▶ Malware comes in many forms, including:
 - ▶ Viruses
 - ▶ Worms
 - ▶ Trojans
 - ▶ Spyware
 - ▶ Adware
 - ▶ Ransomware and scareware

So what is a computer virus? (and what's a worm?!?)

- ▶ A virus is a computer program designed to replicate and damage computer systems and software.
- ▶ To spread between systems, viruses require human action – such as running an executable file, sending an email attachment or copying to and from USB sticks.
- ▶ Worms can spread from machine to machine without any human involvement.
- ▶ Worms are programs that include code to spread using the host computer's file and transport protocols.



Task 1: Research

- ▶ Using Google, find:
 - ▶ 3 examples of computer viruses
 - ▶ 3 examples of computer worms
- ▶ Save them to your P drive folder
 - ▶ Save in a Word file called "malware"
- ▶ You have 5 minutes



5:00

Trojans and adware

- ▶ Trojans are programs that pretend to be something else
 - ▶ Fake games and antivirus are common trojans
- ▶ When run, trojans usually provide a backdoor
 - ▶ A way for attackers to access and monitor the computer
- ▶ Adware displays adverts on the infected computer
 - ▶ To generate sales or click-through revenue
 - ▶ Differs from advertising-supported software as it isn't intentionally installed



Spyware, ransomware & scareware

- ▶ Spyware is malware which monitors computer activity in an attempt to steal passwords or financial information
- ▶ Ransomware is malware which threatens to either delete or publish a user's data unless they pay a fee to unlock it
- ▶ Scareware is malware which incites fear or anxiety to trick a user into buying software, often fake antivirus software

May 2017 WannaCry ransomware

- ▶ Demanded \$300 in BitCoin or would delete user's files
- ▶ Over 200,000 cases in 150 countries
- ▶ Infected UK's NHS computers
- ▶ Lead to hospital appointments being cancelled – including major surgeries
- ▶ Exploited a bug in Windows that had been fixed in March 2017
- ▶ Based on software tools created by the NSA that had been stolen
 - ▶ Tools released to the web for free by hackers on 8 April 2017
- ▶ Combined with a worm to spread it

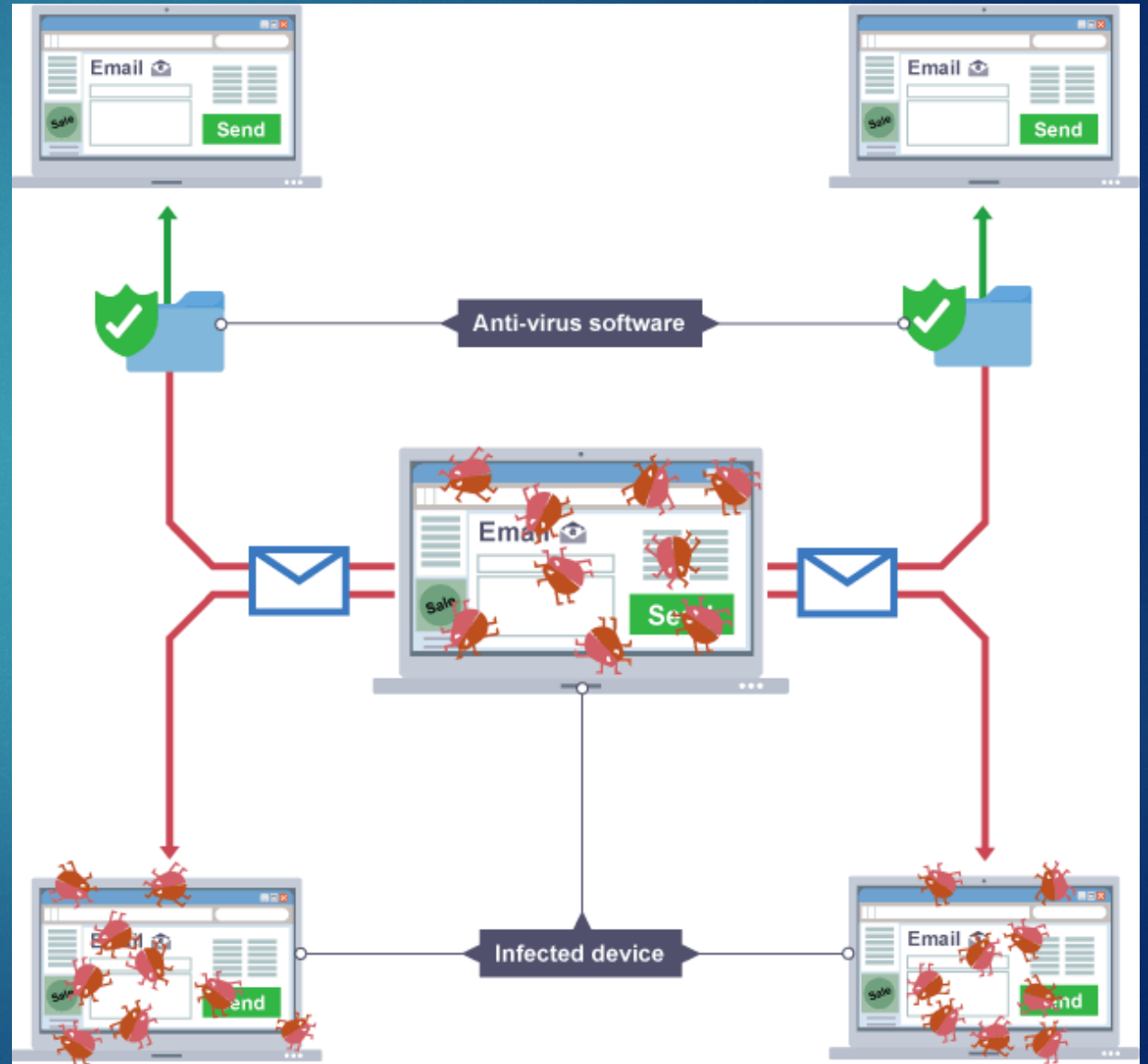


How did this happen?

- ▶ Why did computers become vulnerable to WannaCry?
 - ▶ They hadn't installed operating system updates in 2 months
- ▶ Why was the NHS particularly vulnerable?
 - ▶ Bureaucracy: government bodies make it slow and difficult to update software
- ▶ How was it created?
 - ▶ A hacking group called "The Shadow Brokers" hacked the NSA and stole the tools. They released them to the web for free on 8 April 2017. These tools were then used to create the malware.
- ▶ Why were the tools released for free?
 - ▶ It was released for free as a protest against Donald Trump

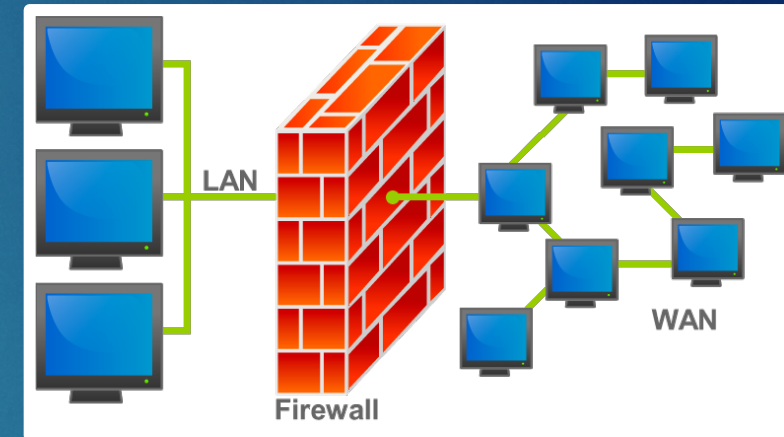
Antivirus software

- ▶ Stops threats spreading from websites, downloads, email attachments and removable media (such as USB sticks)
- ▶ Many can detect and remove spyware, adware and other malware as well as viruses and trojans
- ▶ Popular free antivirus software: AVG, Avast, Bitdefender, Panda, Avira, Malwarebytes



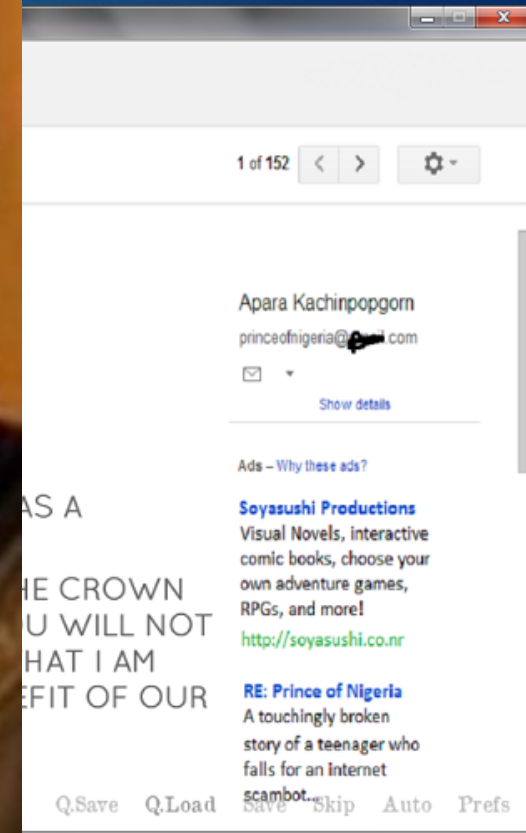
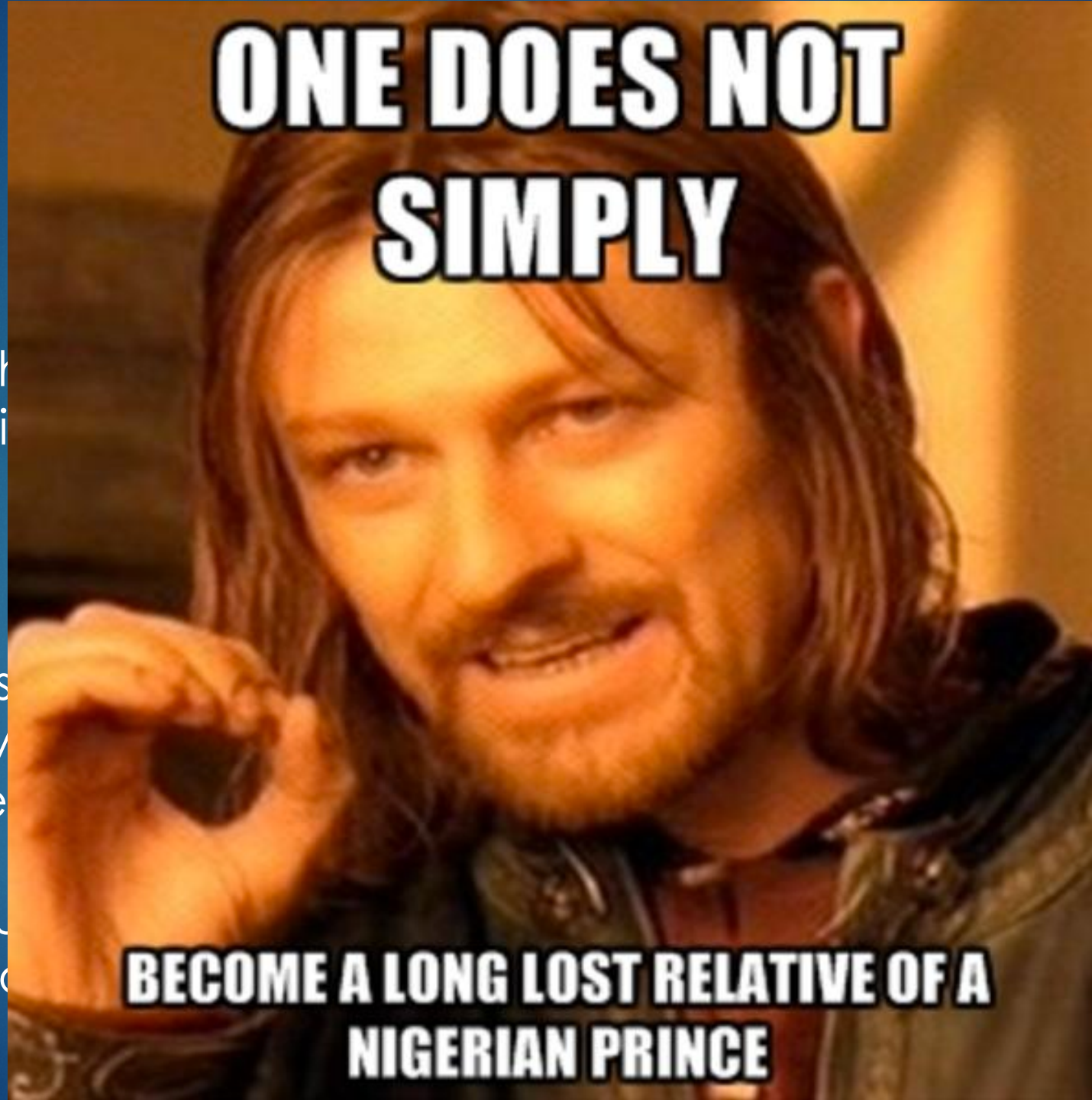
Firewalls

- ▶ A firewall is used to prevent unauthorised communications from a computer
- ▶ Filter traffic by restricting what can pass through
- ▶ Two types:
 - ▶ Hardware firewalls
 - ▶ Software firewalls
- ▶ Hardware firewalls are computers or dedicated machines
- ▶ Software firewalls are applications that run on computers



Greeting

- ▶ Emails that promise something in return, such as sums of money, are often used to transfer money and make it disappear.
- ▶ The classic "prince" scam involves a prince who needs money to cover his expenses and asks you to help him. He can be very charming and will often claim to be a long-lost relative of a Nigerian prince.



Other classic phishing scams

- ▶ Nigerian astronaut
- ▶ Confirm your bank details
- ▶ Confirm your Paypal details

- ▶ Often uses clones of websites (like Apple's online store or Paypal)
- ▶ Often uses slightly misspelled URLs:
 - ▶ paypall.com
 - ▶ store-apple.com

Subject: A really worthy cause which you should be aware of.

Subject: Nigerian Astronaut Wants To Come Home
Dr. Bakare Tunde
Astronautics Project Manager
National Space Research and Development Agency (NASRDA)
Plot 555
Misau Street
PMB 437
Garki, Abuja, FCT NIGERIA

Dear Mr. Sir,

REQUEST FOR ASSISTANCE-STRICTLY CONFIDENTIAL

I am Dr. Bakare Tunde, the cousin of Nigerian Astronaut, Air Force Major Abacha Tunde. He was the first African in space when he made a secret flight to the Salyut 6 space station in 1979. He was on a later Soviet spaceflight, Soyuz T-16Z to the secret Soviet military space station Salyut 8T in 1989. He was stranded there in 1990 when the Soviet Union was dissolved. His other Soviet crew members returned to earth on the Soyuz T-16Z, but his place was taken up by return cargo. There have been occasional Progrez supply flights to keep him going since that time. He is in good humor, but wants to come home.

In the 14-years since he has been on the station, he has accumulated flight pay and interest amounting to almost \$ 15,000,000 American Dollars. This is held in a trust at the Lagos National Savings and Trust Association. If we can obtain access to this money, we can place a down payment with the Russian Space Authorities for a Soyuz return flight to bring him back to Earth. I am told this will cost \$ 3,000,000 American Dollars. In order to access the his trust fund we need your assistance.

Consequently, my colleagues and I are willing to transfer the total amount to your account or subsequent disbursement, since we as civil servants are prohibited by the Code of Conduct Bureau (Civil Service Laws) from opening and/ or operating foreign accounts in our names.

Needless to say, the trust reposed on you at this juncture is enormous. In return, we have agreed to offer you 20 percent of the transferred sum, while 10 percent shall be set aside for incidental expenses (internal and external) between the parties in the course of the transaction. You will be mandated to remit the balance 70 percent to other accounts in due course.

Kindly expedite action as we are behind schedule to enable us include downpayment in this financial quarter.

Please acknowledge the receipt of this message via my direct number [REDACTED] only.

Yours Sincerely, Dr. Bakare Tunde
Astronautics Project Manager

How to avoid phishing scams

- ▶ Legitimate emails never ask you to confirm account details
 - ▶ Don't be fooled
- ▶ If it sounds too good to be true, it probably is
- ▶ Double check destination websites – are they real?
- ▶ Double check the domain name in the sender's email address

Assessment task

- ▶ Grab an iPad
- ▶ Open Kahoot app
- ▶ Using your real name, follow login instructions...

After Half-Term

- ▶ Test!

- ▶ PC Hardware

- ▶ Systems Software and Applications

- ▶ Fetch-Execute Cycle

- ▶ Online Safety

- ▶ In short... **EVERYTHING** we've covered this half term
(apart from Assembly Language)

- ▶ **Your November report will be based on your performance on this test**