HOW TO STAY SAFE IN THE DIGITAL AGE

A QUICK GUIDE

THE GOOD NEWS

- A computer is just a tool, so there is no need to be afraid of it. You can always turn it off. If you break it, it can usually be fixed.
- You can do lots of fun things on a computer.
- You do not need to be a victim of computer crime or fraud if you use your common sense.

PROTECTING YOUR DEVICE ON THE INTERNET

- 1: Always make sure you have a firewall. Windows has an in-built firewall. To find out follow this link

https://www.computerhope.com/issues/ch000551.htm

- 2: Always make sure you have anti-virus software. Windows has an inbuilt antivirus either called Windows Defender or Microsoft Security Essentials. To find out more follow this link.

http://www.itpro.co.uk/desktop-software/26635/how-to-turn-on-windows-defender-1

There are also a number of free antivirus programs. (Mobile Phones also need anti-virus)

http://www.techadvisor.co.uk/test-centre/security/best-antivirus-2017-free-paid-antivirus-reviews-3651652/

- 3: Enable automatic download and installation of operating system and anti-virus updates.

https://www.lifewire.com/how-to-change-windows-update-settings-2625778

PROTECTING YOUR COMPUTER ON THE INTERNET

- Install an anti-malware program.

http://www.techradar.com/news/software/applications/best-free-anti-spyware-and-anti-malware-software-1321656

- 4: Make sure you always back up your files regularly. This will ensure that if something goes wrong Windows has a built in back up solution that you can schedule to back up automatically. Alternatively you will need a backup program. A selection of free programs is shown in the link below:

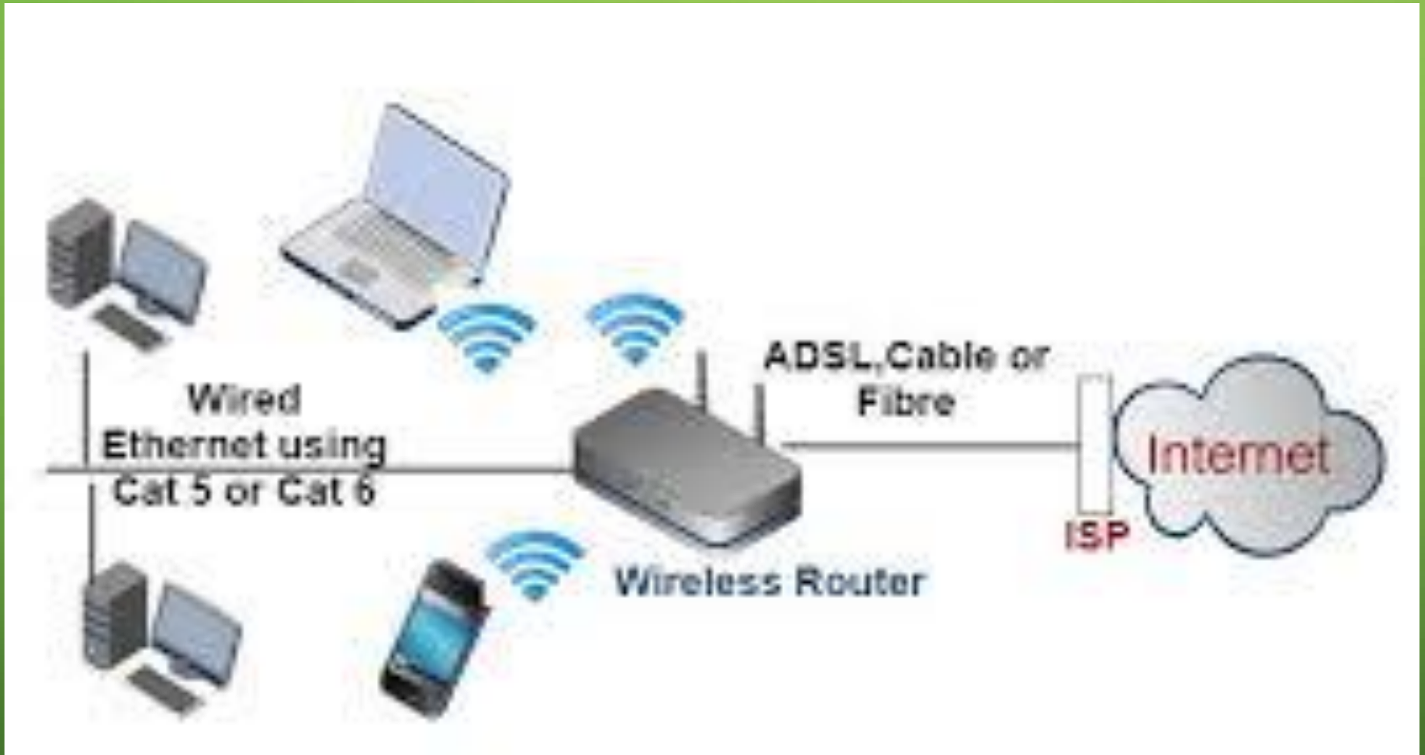
http://www.techradar.com/news/the-best-free-pc-backup-software

- 5. Don’t use the same password for all your online accounts and have a strong password. If you have trouble remembering passwords, use a password safe program such as Keepass or Lastpass.
- Whilst people have different opinions about what is best, these steps are sufficient for most people.

YOU CAN PREVENT MOST PROBLEMS BY BEING VIGILANT

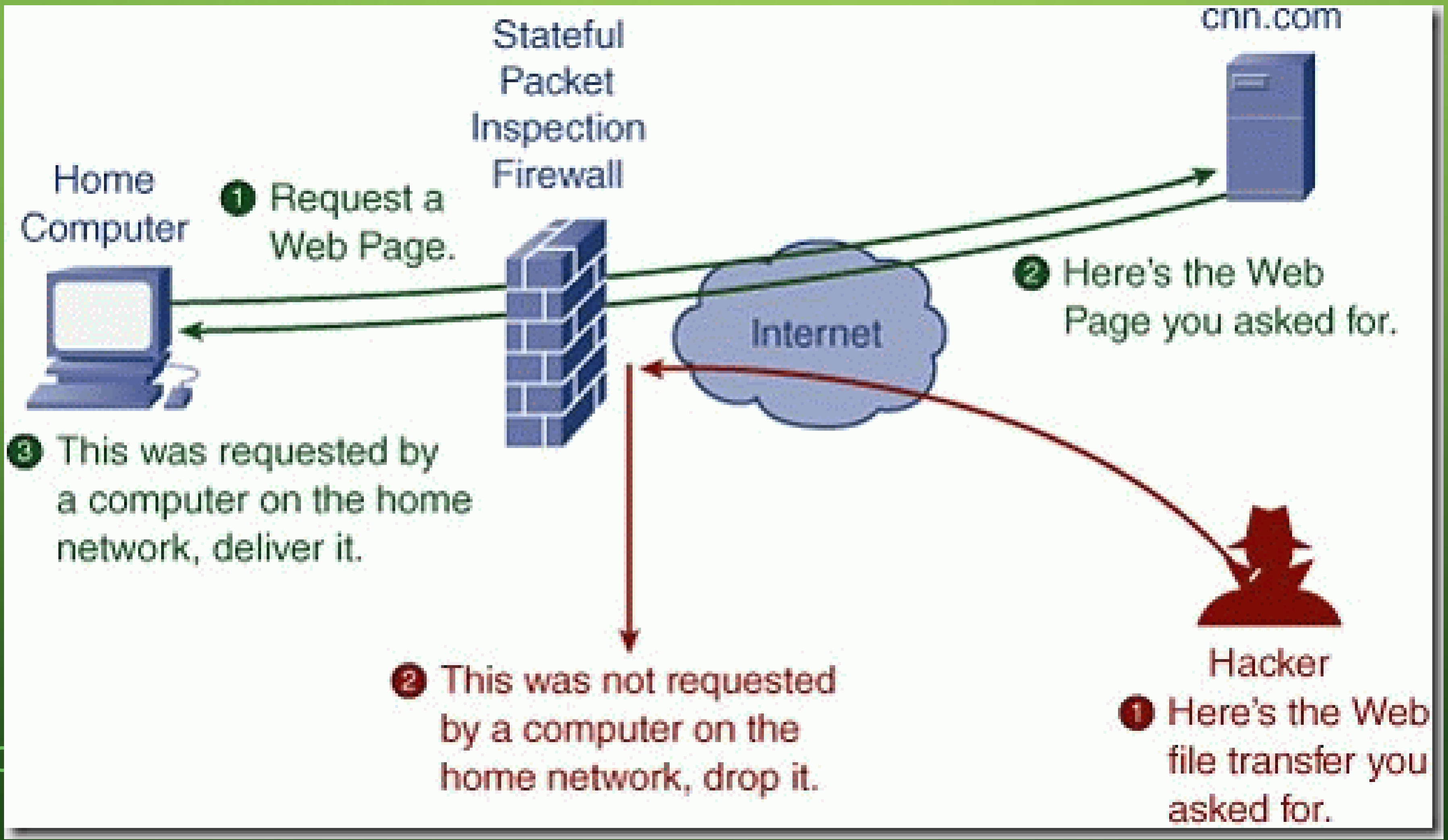
- There are four primary methods by which your information might be obtained and fraudulently used.
- 1). You go to a website and click on a link or a pop up that downloads a rogue program onto your computer.
- 2). You receive an email and you inadvertently carry out an action that compromises your computer.
- 3). You download and install a program from an untrusted site.
- 4). You send sensitive information via an insecure public Wi-fi hotspot.
- This can lead to any information including passwords and bank details being stolen from your computer, and malicious software being sent to all your friends and contacts.

TYPICAL HOME NETWORK



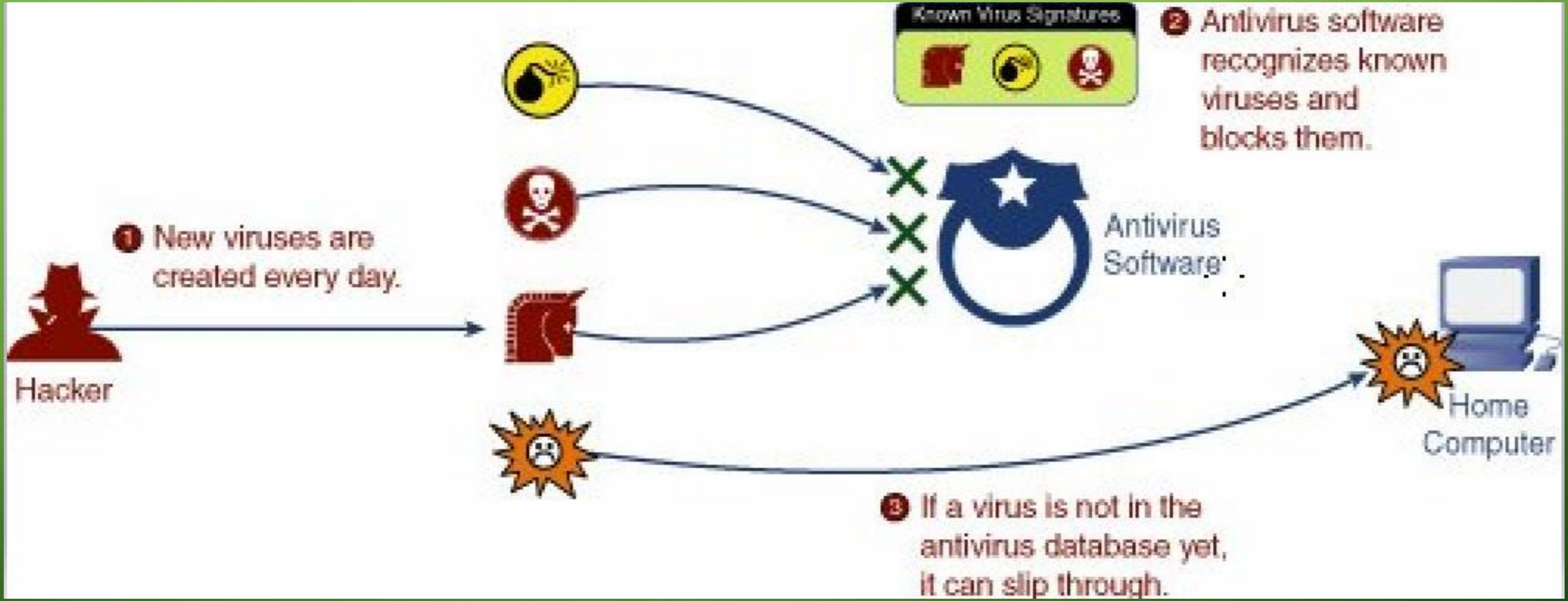
Network Diagram-Typical Simple Home Network

WHAT DOES A FIREWALL DO



cnn.com
Stateful Packet Inspection Firewall
Home Computer
1 Request a Web Page.
2 Here's the Web Page you asked for.
Internet
3 This was requested by a computer on the home network, deliver it.
2 This was not requested by a computer on the home network, drop it.
Hacker
1 Here's the Web file transfer you asked for.

WHAT DOES AN ANTI-VIRUS PROGRAM DO



Known Virus Signatures
2 Antivirus software recognizes known viruses and blocks them.
1 New viruses are created every day.
Hacker
Antivirus Software
Home Computer
3 If a virus is not in the antivirus database yet, it can slip through.

What to do if you get a virus on your computer

WHAT IS THE DIFFERENCE BETWEEN ANTI MALWARE AND ANTI VIRUS

- Antivirus usually deals with the older, more established threats, such as Trojans, viruses, and worms.
- Anti-malware, by contrast, typically focuses on newer stuff, such as malware delivered by zero-day exploits (new threats with no Anti-Virus definition).
- Antivirus protects users from lingering, predictable-yet-still-dangerous malware.
- Anti-malware protects users from the latest, currently in the wild, and even more dangerous threats making it the best protection against new malware you might encounter while surfing the net.
- Antivirus is best at crushing malware you might contract from a traditional source, like a USB or an email attachment.
- How to clean an infected computer

PREVENTING WEBSITE FRAUD

- 1: Keep your operating system and anti-virus software up to date using the automatic update option.
- 2: Make sure that when you visit a website that the site address in the address bar is spelled correctly. Fraudsters can make excellent copies of genuine websites. http://www.which.co.uk/consumer-rights/advice/how-to-spot-a-fake-fraudulent-or-scam-website
- 3: Do not click on any pop-up messages on any website that you do not know to be safe. Do not trust messages that claim that something is wrong and never click on the pop-up to fix it. If you are concerned about what you see on the screen, and cannot close the pop up, shut down your computer.
- 4: If you don't know the website to be genuine and if an offer seems too good to be true, it almost certainly is. The goods are either counterfeit or a trap to get you to click on a harmful link.

PREVENTING EMAIL ATTACKS

- 90% of computers that have been compromised have been compromised because the recipient of an email has acted inappropriately.
- Generally no company is going to request that you tell them financial details and confidential information by email or phone. They will use mail. As a general rule disclose as little as possible when on the Internet, and that includes on social media.
- Fraudsters send fake emails that look genuine and appear to have come from a trusted source such as someone you know or a company you trust.
- The email may have an attachment or a link to a website that looks genuine and may include the logos and graphics of a trusted company.

SUSPICIOUS THINGS TO LOOK OUT FOR

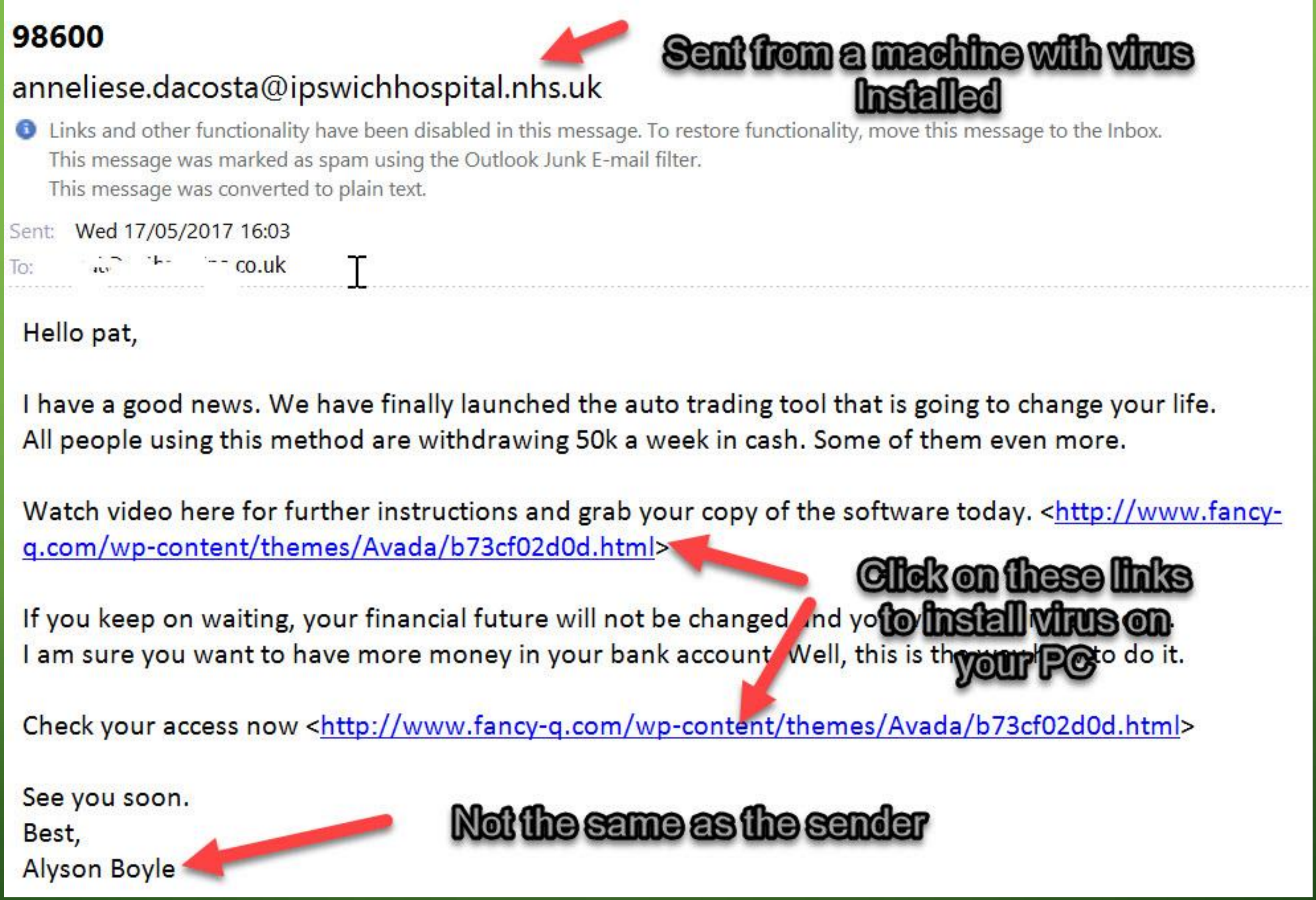
- 1: The email contains content that appeals to your greed telling you that you have won some kind of reward or can do so by responding to the mail or by clicking a link in the email. This is an obvious fraud and should be deleted.
- 2: The email has text that indicates that some urgent action is required on your part that seems to be sent by a financial services provider like a bank or a company that you know and trust.
- The email is from someone you don't know.
- The email content is in poor English or badly spelled.
- The email appears to be from someone you know and contains links or attachments.
- The email has an attachment with text suggesting that you need to open it for some reason.
- The email is unexpected.

THINGS TO AVOID DOING

- 1: Do not click on any links in emails that you do not trust.
- 2. Do not open any attachments that you are not expecting, regardless of who appears to have sent the email.
- You do not have to open any email. You can delete any or all you choose. If an email concerns you, check with the sender if you know them. Do not reply to the email.
- If you are worried about email spam, you can download MailWasher Free from http://www.mailwasher.net/

OTHER GENERAL ADVICE

- There is a fraud where people telephone you claiming to be from Microsoft or some other company and telling you that they can see that your computer has some fault. They then persuade you to log on to a website to get the “fault fixed” and charge you for doing so. What they claim is not possible and is a con trick, regardless of how much information you think they know about you.
- Telephone or door to door cold calling. If you have not requested contact from someone, put the phone down or close the door. There is no need to be polite. They are invading your privacy.



98600

anneliese.dacosta@ipswichhospital.nhs.uk

Links and other functionality have been disabled in this message. To restore functionality, move this message to the Inbox.
This message was marked as spam using the Outlook Junk E-mail filter.
This message was converted to plain text.

Sent: Wed 17/05/2017 16:03
To: [redacted] co.uk

Hello pat,

I have a good news. We have finally launched the auto trading tool that is going to change your life.
All people using this method are withdrawing 50k a week in cash. Some of them even more.

Watch video here for further instructions and grab your copy of the software today. <http://www.fancy-q.com/wp-content/themes/Avada/b73cf02d0d.html>

If you keep on waiting, your financial future will not be changed and yo
I am sure you want to have more money in your bank account. Well, this is th to do it.

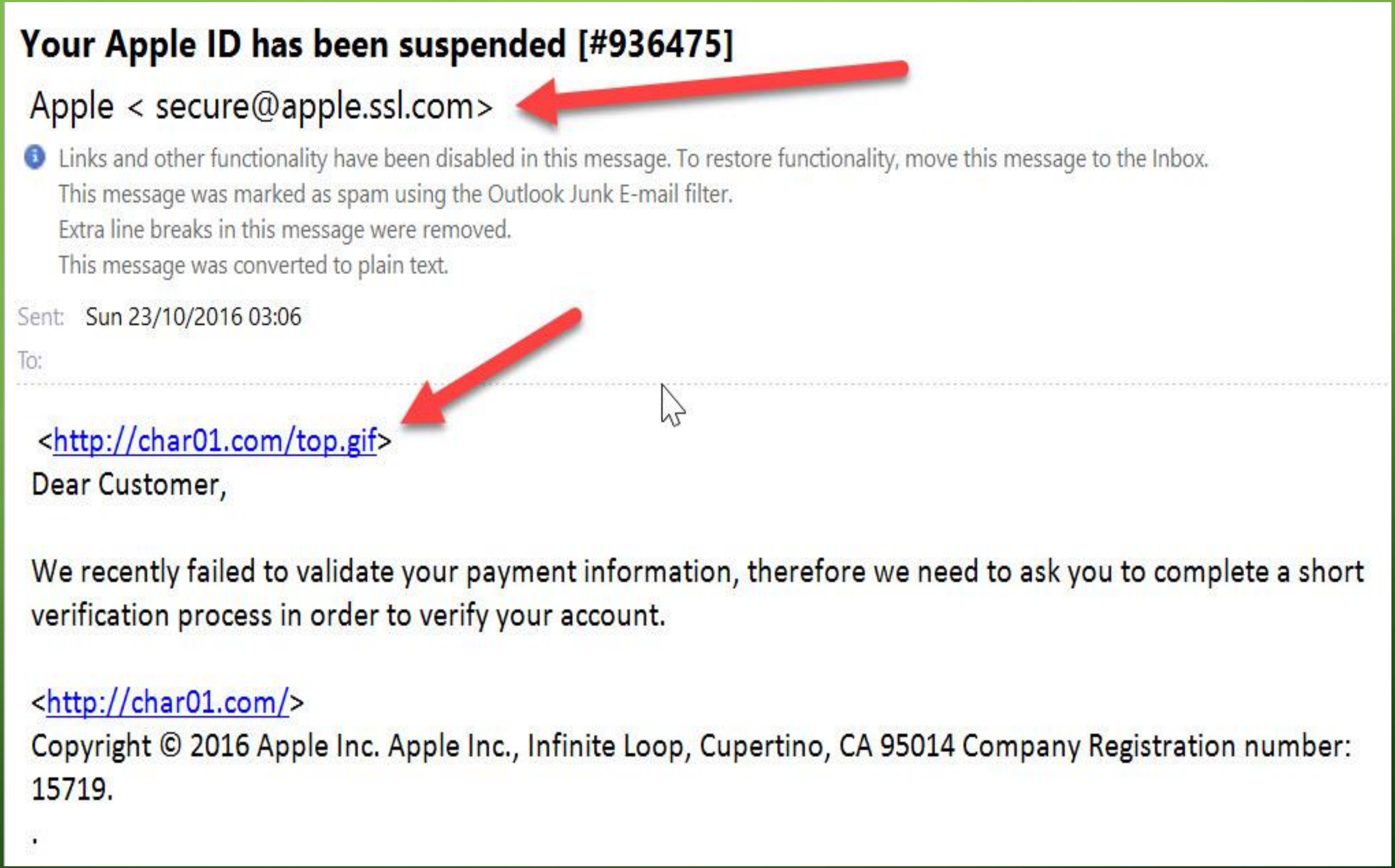
Check your access now <http://www.fancy-q.com/wp-content/themes/Avada/b73cf02d0d.html>

See you soon.
Best,
Alyson Boyle

Sent from a machine with virus Installed

Click on these links to install virus on your PC

Not the same as the sender



Your Apple ID has been suspended [#936475]

Apple < secure@apple.ssl.com>

Links and other functionality have been disabled in this message. To restore functionality, move this message to the Inbox.
This message was marked as spam using the Outlook Junk E-mail filter.
Extra line breaks in this message were removed.
This message was converted to plain text.

Sent: Sun 23/10/2016 03:06
To:

<http://char01.com/top.gif>
Dear Customer,

We recently failed to validate your payment information, therefore we need to ask you to complete a short verification process in order to verify your account.

<http://char01.com/>
Copyright © 2016 Apple Inc. Apple Inc., Infinite Loop, Cupertino, CA 95014 Company Registration number: 15719.

.

MOST SUCCESSFUL EMAIL SCAM TITLES

- SECURITY ALERT 21%
- REVISED VACATION & SICK TIME POLICY 14%
- UPS LABEL DELIVERY 1ZBE312TNY00015011 10%
- BREAKING: UNITED AIRLINES PASSENGER DIES FROM BRAIN HEMORRHAGE - VIDEO 10%
- A DELIVERY ATTEMPT WAS MADE 10%
- ALL EMPLOYEES: UPDATE YOUR HEALTHCARE INFO 9%
- CHANGE OF PASSWORD REQUIRED IMMEDIATELY 8%
- PASSWORD CHECK REQUIRED IMMEDIATELY 7%
- UNUSUAL SIGN-IN ACTIVITY 6%
- URGENT ACTION REQUIRED 6%

HELPING YOURSELF

- Searching the internet will often give you the answer.
- When searching just use the important words e.g Best free Apple PC antivirus.
- Verify a product by looking for reviews e.g. Kaspersky antivirus for Apple Mac review. Look for articles that look like the type of result you are expecting. These will not always be the first result in the search results list.
- If you don’t understand what you are reading, ask a trusted young person.

CONCLUSION

- Make sure your computer has a firewall and anti-virus program and smart phones have an anti-virus program.
- Be cautious about clicking on links in email and on unknown websites.
- Do not install software that you do not know to be safe.
- Do not carry out any financial transactions on public wi-fi networks.
- Be smart and stay safe. Your safety is mainly under your control.
- https://www.getsafeonline.org/