Bristol Brunel Academy,
Speedwell Road, Speedwell, Bristol BS15 1NU
Tel: 0117 377 2700 Fax: 0117 377 2701

Email: info@bba.bristol.sch.uk
Website: www.bba.bristol.sch.uk
Principal: Mr J Jones

Bristol Brunel Academy

December 2020

Dear Parent/Carer,

As E-Safety lead, I have been working closely with Avon and Somerset Police Cyber team in organising a virtual event on Eventbrite for parents, where they will be talking about the online gaming, cybercrimes and how to protect from attacks. The event will cover the seriousness of these cyber-attacks, in particular Denial of Service (DoS) attacks, but also the measures that people can put in place to ensure they don't become a victim.

The event is on Thursday 17th December, 12:30pm – 13:30pm.

Please find the below letter on behalf of Avon and Somerset Police, explaining about Denial of Service (DoS) attacks and the legalisation around cyber-attacks.

What is a DoS or DDoS Attack and how do they effect Gamers?

A Denial of Service (DoS) attack, is a cyber-attack carried by an individual to shut down a machine or network (DENIAL), which ultimately prevents you from using a particular service (of SERVICE).

It is carried out by sending 'unwanted traffic' to a target IP address, which subsequently overwhelms it with data, resulting in the network appearing offline, or perhaps slowing it down so much it renders it unusable. Usually, attacks on individual gamers are carried using a simple denial of service attack but as one network connection is unlikely to be able to send enough data to properly 'flood' its target alone, attackers may use a distributed denial of service (DDoS) attack instead.

In a DDoS attacks, multiple computers (Distributed) are used to carry out the DoS and flood the target IP address. This is typically done by using a group of computers also known as a botnet, which have been infected by malware allowing attackers to initiate network traffic from those devices - often without the owner's knowledge or awareness.

The Law and the Computer Misuse Act 1990

The CMA is a key piece of legislation that criminalises the act of accessing or modifying data stored on a computer system without appropriate consent or permission. It has been amended to create a new offence for unauthorised acts. Section 3: Unauthorised Acts with intent to impair, or with recklessness as to impairing the operation of a computer. This offense covers intentionally, or recklessly, introducing malware to other people's systems or a DoS/DDoS attack - the maximum sentence on indictment is 10 years imprisonment.

How do you know you are being DoSed and what actions should be taken?

You may experience a sudden outage or unexplained loss in connection. However, most Internet Service Providers (ISPs) will have some form of outages over a given year so it is important to isolate that it isn't a normal network outage. Alternatively, someone may have threatened to 'boot you offline' in an online game – this is usually the case.

The first thing to do is unplug your router, both at the power and broadband cable. This should be followed by turning off your device such as your computer or gaming console and leaving it off for a period of time. Please note that this 'period of time' is dependent on the ISP's configuration.

If your connection has not been restored, you should be able to check outages in your area using a mobile device (on a data plan) by heading to your ISP's website. If it appears like there is no outages in your area you can call your ISP

and ask them to investigate the outage - they may be able to see suspicious traffic heading to your network confirming a DoS attack is in motion.

So how do you stop the DoS?

Obtaining a new IP address is easiest and most effective way to stop an ongoing attack, since attack is carried out automatically on a specific IP address. In order to change your IP, you will need to:

1. Unplug your router - there is no timescale on how long this will take to change as all ISP leases are different, it could be anywhere from 10 minutes to 12 hours.

2. Log into your router (if possible) - some ISP's have functionality to reset your IP address by visiting the Admin Console (usually https//:192.168.1.1) and looking under 'Network Settings' - if the ISP allows it there should be some guide on how to successfully change your IP address.

3. Contact your ISP - request a new IP as you suspect your IP is being targeted as part of a DoS attack, they may be able to assist you with changing the lease.

Preventing a DoS in the first place.

1. Antivirus and firewall - make sure your own devices don't become infected by a Trojan virus and turn into members of a botnet themselves. Make sure you have a firewall and antivirus installed on all computers connected to your network, and be sure to configure your security software to automatically download important updates.

2. VPN - a Virtual Private Network (VPN) effectively hides your IP address behind a virtual wall. Attackers looking for your IP address will only see the VPN's IP. Assuming they carry out the attack, the DoS traffic will hit your VPN's servers first, where it will be screened out before reaching your home network. There are downsides of a VPN, mainly it's the lack of control and the fact you are relying on your VPN provider's procedures. Additionally, a VPN adds an extra step, which can of course lead to latency and higher ping times in-game. It's best to stick with providers that can guarantee security as well as speed. Thorough research is needed!

3. Upgrade your home network - some routers and hardware firewalls are available with built-in safeguards against DDoS attacks and other network intrusions – again research is needed.

If you struggle with technical information and need help with implementing some of the measures above - you can use websites like https://www.howtogeek.com/ and https://www.lifewire.com/

A DoS or DDoS attack don't necessarily require understanding or sophisticated individuals to carry them out effectively. Most of the time a DoS is used by an angry gamer as a retaliation following an online multiplayer game but they don't truly understand what they are doing is breaking the law. Talking to children about this type of attacks is essential.

Kind regards

Drew Jefferies
Cyber Protect Officer