CRIMES OF THE CYBER SPACE

Many songs of praise can be sung about how the internet has revolutionised our lives. From bridging people across the globe, to opening new platforms for sharing ideas, it has undoubtedly made tremendous contributions to social and technological advancements.

However, as is the norm with any great human creation, this tool of advancement has also become a breeding ground for a new kind of menace. In much the same way that lawlessness riddles our society, crime, it seems, has also found its way into the cyberspace.

Dubbed 'cybercrime', the term is everywhere and on everyone's lips, but what does 'cybercrime' really mean?

The common definition for the term is any crime that involves a computer and a network. The computer may have been used in the committing of a crime, or it may be the target. Offences committed against individuals with a criminal motive using modern telecommunication networks such as the internet and mobile phones falls under the jurisdiction of cybercrime.

What all this actually means, in case all those long words makes no sense, is that someone from across the world has the ability to either steal your money, your information, or in fact, your very identity. Hard to imagine, but that is a very small example of a problem rampant on a much larger scale.

Even though Bangladesh joined the internet age in the late 90s, it has been shown no quarter, and as such, cybercrime is quite actively present here.

HACKING

A term feared by any and all electronic users, hacking is essentially gaining unauthorised access to a system or network for the purposes of stealing or manipulating information.

MALWARE DISTRIBUTION

This term may seem foreign to normal users, but alarmingly a very big segment of cyber problem falls under its jurisdiction, more simply known as – virus!

The greatly feared computer virus is just one of the many forms of malware out there. And each type has its own specialty. Some can be used to spy on users, while others are designed to quietly steal information, or be used to control your electronics. And many of these can even replicate itself in your machine and then use your contact list to spread to other unsuspecting users.

PIRACY

This is a worldwide problem, causing problems throughout the industry, both the entertainment industries and to companies that develop paid software. Unfortunately, this is a problem for our country as well, and it has the same negative impacts elsewhere in the world.

CYBER BULLYING AND EXTORTION SCHEMES

This encompasses a large number of crimes that perpetrators can pull against their victims. Cyber bullying, for example, is when the criminal harass their victims in the realms of cyberspace, through social media, or through specifically created web pages or chain mail, etc. Then there are the many extortion schemes. Some come in the façade of an email or link claim

ing to be some competition prize confirmation and the unfortunate thing is, it works quite well.

Unsuspecting users, believing they have won something, spend no time thinking, and end up victims of either having their money, personal information, or their identity stolen. If the attacker finds something of interest, they can then ask for ransom. There can also be threats made to someone by a criminal. It is the easiest way, because the threat can be delivered without leaving any trace and staying completely anonymous.

PHISHING

Imagine sitting in front of a computer, accessing the log-in page of Facebook, providing your email address and password and clicking sign in, but it does not happen. So you repeat the process and you finally log in. An hour or so later, when you try to log back into Facebook for something, you find that you cannot access your account regardless of how many times you check your password as you type. Possibly, you have just become the latest victim of phishing!

This way perpetrators obtain any and all information by posing as a trustworthy webpage wrapper, waiting for an unsuspecting victim to spring the trap. This method is used to steal credit card details, accounts, etc. This is a favourite method for criminals to commit credit card fraud and identity theft.

CYBERCRIME AGAINST WOMEN

This is, quite possibly, the most frequent and rampant variant of cybercrime that happens in your country. Crimes include threatening or harassing, hacking sensitive information and then asking for ransom, using a normal picture of the victim, then morphing it and attempting to extort ransom and of course, uploading sensitive private videos of them on the internet.

Most of these crimes are committed with the main motivations being either revenge for some baseless grudge or money. Social media sites such as Facebook, Twitter, Instagram, etc. are also a minefield of criminal traps if you are not careful. All the above listed crimes take place here too and it is a better place to find easy to fool users.

WAYS OF PREVENTION

There are of course things you can do to stay safe in the cyberspace to a large extent. Some simple tips include:

Use strong passwords, and change them as often as possible. This can be achieved by using a combination of letters, symbols and numbers to form a unique password.

Secure your computer through advanced security system software. There are plenty of system protection software available from the likes of Eset, Avast, Kaspersky, etc. which are designed to automatically take care of everything in the background while you work.

Avoid filling out personal information on random or untrustworthy sites. If you happen to browsing for something and end up in a website where it asks for your details, please make sure the website is reputable, and has any connection to the activity you are currently engaged in to end up at that website.

ENCRYPT SPECIFIC PERSONAL DATA WITH PASSWORDS

While it is impossible to encrypt everything, at least protect information like National ID copies, passports, banking information and others. Winrar is a very common application that you can use to apply strict encrypting and password protection to these valuable data.

AVOID CLICKING ON EMAILS WITH DUBIOUS CONTENTS AND LINKS

Emails stating that you have just won $10,000,000 are obviously a trap. So are the other similar emails that state something outlandish. Avoid these at all costs. When logging in from other computers or devices, use the incognito option to keep your browsing history and any other information from being stored.

While all this information may cast a bleak picture of the cyberspace, and cast the internet in a very bad light, do remember that the internet has done a lot to contribute to society and will continue to do so for years to some. It is a wondrous place and an invaluable tool, and if used correctly and carefully, that experience will stay that way.

If you feel that you are a victim of cybercrime, please understand that the first order of business is to go to the right people for help. Going to the wrong people for assistance will only worsen the situation. Our country already has an established active cybercrimes division, dealing with such cybercrime issues. So the first thing to do if you have fallen victim to cybercrime is to contact RAB (Rapid Action Battalion). Please visit RAB's website http://www.rab.gov.bd/english/report-crime-2/ and report the crime or call their Operations Control Room 01777720029.

By Intisab Shahriyar
Photo: Collected