Cybercrime

In the 21st century, living a lifestyle has developed lately. It allowed people to make communication, interaction, and interactive online communication. Moreover, the way that we communicate has been used for different purposes such as education, learning, working, connecting, collaboration, and advancing technology. However, no matter what the issue usually happens in one society and then becomes a country issue and moves to a global issue. On the other hand, during the covid-19 pandemic, everything is flexible. We have transformed from studying physically into virtually, working physically into virtually for any purposes like business, government, or political. Unfortunately, using the internet can be both rewarding and challenging. For instance, a cybercriminal is a person who conducts some form of illegal activity using computers or other digital technology such as the Internet.

Most cybercrime is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. In other words, in the digital age our virtual identities are essential elements of everyday life: we are a bundle of numbers and identifiers in multiple computer database owned by governments and corporations. Cybercrime highlights the centrality of networked computers in our lives, as well as the fragility of such seemingly solid facts as individual identity. Before going further, what is the purpose of doing that? Cybercrime? Because criminals sell stolen information, criminals can operate anywhere. However, there are different types of cyber crimes such as identity theft, invasion of privacy, internet fraud, email hacking, computer viruses, spam, theft of financial or card payment data, the use of confusingly similar domain names for criminal purposes, cybersquatting and so on. The term **cybersquatting** refers to the unauthorized registration and use of Internet domain names that are identical or similar to trademarks, service marks, company names, or personal names. Cybersquatting registrants obtain and use the domain name with the bad faith intent to profit from the goodwill of the actual trademark owner. Both the federal government and the Internet Corporation for Assigned Names and Numbers have taken action to protect the owners of trademarks and businesses against cybersquatting abuses. There are four types of cybersquatting. First of all, typosquatting is to trick Internet users, typosquatters may also create a fake website that resembles the source by using a similar layout, color schemes, logos, and content. Typosquatters use such fake websites to compel legitimate website owners to buy the cybersquatting domain names, generate more web traffic, and spread malware. Second, identity theft. Third, name jacking. Name jacking refers to the registration of a domain name associated with the name of an individual, usually celebrities and well-known public figures. Name jackers benefit from web traffic related to the targeted individuals. Lastly, reverse cybersquatting. Cybersquatting has become a lucrative online practice that may negatively affect the reputation of well-established commercial brands. The owners of such brands may face legal challenges related to overcoming their cybersquatting issues. This is because the demarcation line between the legality and

illegality of cybersquatting is difficult to draw, as the phenomenon combines both legitimate and illegal activities. By the way, how does cybersquatting affect the owner and user on the website?

Although domain name disputes related to cybersquatting and related practices can be resolved in a timely and affordable manner through UDRP procedures, preventive measures can save trademarks owners the fees for initiating such procedures. Besides that, The SSAC engages in ongoing threat assessment and risk analysis of the Internet naming and address allocation services to assess where the principal threats to stability and security lie, and advises the ICANN community accordingly. How does SSAC operate? SSAC members are skilled and experienced technical professionals who volunteer their time and expertise to improve the security and integrity of the Internet's naming and addressing system. The SSAC produces Reports, Correspondence, and Comments on a range of topics. Reports are focused on providing information, recommendations and advice on technical Security Stability and Reliability (SSR) issues to the ICANN Board, the ICANN community, and/or the broader internet community. Correspondence comprises letters, comments and other documents on administrative, community and other non-SSR issues. Comments are prepared in response to explicit questions posed to or requests made to the SSAC, or as a response to ICANN's public comment forum.

In conclusion, cybercrime and cybersquatting are still concerns for the world internet. Although we are living in the internet lifestyle, we still need stability and internet security for any purposes of using the internet.