Cyber Security

cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It is also known as information technology security or electronic information security. Also, it is the protection of internet-connected system such as hardware, software, and data from cyberthreats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and computerized systems.

As technology has revolutionized Nepal in the past few years, the associated crimes committed using technology have also increased. News and reports of cyber security breaches had been regularly broadcasted to the public many times in the past and recent days by the Medias and Police department. It has been very risky and challenging critical IT environment Nepal faces today despite their high regard for security and privacy, relevant policies regarding cyber security in Nepal are still not able to address the growing security breach concerns of the cyber users.

Nepal is specialized in Web and mobile apps development in which they have a lot of new startups. Big companies like Verisk, Leapfrog and other companies in Nepal are providing services for the other companies Europe, America, and other countries of Asia.

Some Cyber security Breach are:

Equifax

in 2017, a website application vulnerability caused the company to lose the personal details of 145 million Americans. This included their names, SSNs, and drivers' license numbers. The attacks were made over a three-month period from May to July, but the security breach wasn't announced until September.

Yahoo

Yahoo disclosed that a breach in August 2013 by a group of hackers had compromised 1 billion accounts. In this instance, security questions and answers were also compromised, increasing the risk of identity theft. The breach was first reported by Yahoo while in negotiations to sell itself to Verizon, on December 14, 2016. Yahoo forced all affected users to change passwords and to reenter any unencrypted security questions and answers to re-encrypt them.

Facebook

In April 2019, the Up Guard Cyber Risk team revealed two third-party Facebook app datasets had been exposed to the public Internet. One, originating from the Mexico-based media company Culture, weighs in at 146 gigabytes and contains over 533 million records detailing comments, likes, reactions, account names, FB IDs and more. This same type of collection, in similarly concentrated form, has been cause for concern in the recent past, given the potential uses of such data.

Dating site

It is marketed itself to married people wishing to have affairs, was hacked in 2015. The hackers went on to leak a huge number of customer details via the internet. Extortionists began to target customers whose names were leaked; unconfirmed reports have linked several suicides to exposure by the data breach.

Twitter

In May of 2018, social media giant twitter notified users of a glitch that stored passwords unmasked in an internal log, making all user passwords accessible to the internal network. Twitter told its 330 million users to change their passwords, but the company said it fixed the bug and that there was no indication of a breach or misuse but encouraged the password update as a precaution. Twitter did not disclose how many users were impacted but indicated that the number of users was significant and that they were exposed for several months.