**History’s real time cyber attacks:**

### **NASA Cyber Attack:**

**Procedure:**

A 15-year-old boy named Jonathan James, who operated under the name 'c0mrade' hacked the computers of the Department of Defense and NASA, causing a 21-day shutdown of NASA computers that supported the ISS (International Space Station).

The NASA cyberattack is a reminder that no organization is immune to attack. It is important for all organizations to take steps to protect their computer systems and data. By following the tips mentioned above, you can help to protect your organization from cyberattacks.

**Introduction:**

The NASA cyber attack in 1999 was a significant event in the history of cybersecurity. It was one of the first high-profile cyberattacks against a government agency, and it highlighted the vulnerability of even the most secure computer systems.

### **The 2007 Estonia Cyber Attack:**

**Procedure:**

There is significant debate among experts regarding the definition of cyberwarfare, and even if such a thing exists. One view is that the term is a misnomer since no cyber attacks to date could be described as a war. An alternative view is that it is a suitable label for cyber attacks which cause physical damage to people and objects in the real world.

**Introduction:**

In the spring of 2007 Estonia fell under a cyber attack campaign lasting a total of 22 days. The attacks were part of a wider political conflict between Estonia and Russia over the relocation of a Soviet-era monument in Tallinn. Due to the lack of definitive quantitative data, the author will use qualitative analysis to explain the cyber attacks.

### **A Cyber Attack on Marriott Hotels :**

**Procedure:**

Investigators began scouring the system for clues, and discovered a Remote Access Trojan (RAT) along with MimiKatz, a tool for sniffing out username/password combos in system memory. Together, these two tools could have given the attackers control of the administrator account.

Is not clear how the RAT was placed onto the Starwood server, but such [Trojans](https://www.csoonline.com/article/567385/what-is-a-trojan-horse-how-this-tricky-malware-works.html) are often downloaded from [phishing](https://www.csoonline.com/article/514515/what-is-phishing-examples-types-and-techniques.html) emails, and it’s [reasonable to guess that might’ve been the case here](https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/).

**Introduction:**

The cyber attack on Marriott International in November 2018 was a major data breach that exposed the personal information of millions of guests. Here's a detailed breakdown of what happened: Timeline: 2014: Attackers gained unauthorized access to the Starwood Hotels network, which Marriott acquired in 2016.

### **The biggest password leak yet:**

**Procedure:**

Passwords Leaked: A file with around 10 billion (1,000 crores) passwords was leaked via an online hacking forum, according to a report by Semafor. The compilation, which included old and new password breaches, was posted online on July 4 and is the largest such leak yet, the report added.

* Ensure you use different passwords for different platforms wherever possible, especially for sensitive accounts linked to banks, insurance, and other financials.
* Create strong eight- to twelve-character passwords with at least one capital letter, one numeral, and one symbol.
* Do not share your passwords with anyone or write them down so that others can hack or access them.
* Change your passwords and pins regularly and ensure they are completely different.

**Introduction:**

The RockYou2024 leaked password database is a serious security risk; it contains almost 10 billion account credentials. This unprecedented leak further increases the exposure to credential stuffing, brute force and password cracking attacks.