Berif study of Cyberattacks in Nepal

**INTRODUCTION**

Nowadays, cyberattacks are becoming increasingly common in Nepal, largely due to a lack of awareness and knowledge about technology. While people use smartphones, they often do not use them smartly or securely. Hackers use various methods to hack devices, such as **Man-in-the-Middle (MITM) attacks, Distributed Denial of Service (DDoS), Phis hing, Social Engineering, Voice Calling, Message-Based Vectors, Image-Based Vectors, and Exploiting Vulnerable Software.** These attacks target devices like **smartphones, computers, servers, and IP phones** to steal **sensitive information, including names, email addresses, contact numbers, social media details, qualifications, and educational backgrounds.**

Some **hackers carry out attacks for entertainment, while others do it for blackmail or financial gain. Every hacker has their own motives and perspective for hacking.** Unfortunately, even government systems have not been spared, with several incidents of cybercrime reported in recent years. These incidents highlight the urgent need for better cybersecurity awareness and measures to protect individuals and institutions from such threats.

In recent years, cyberattacks have become a major threat to businesses and individuals in Nepal. This article aims to explain what cybersecurity and cyberattacks are, and it provides a brief look at some cyberattacks that have happened in Nepal. It also explains the reasons behind these attacks, their effects, and how to deal with them. Additionally, the article talks about ways to prevent cyberattacks and how to respond if an attack happens.

By the end of this class, students will have a clearer understanding of the current situation of cyberattacks in Nepal and how to protect themselves from such threats. This seminar is designed for business owners, IT professionals, and anyone who wants to stay safe online. As more government services and businesses move online, the risk of cyberattacks in Nepal is growing. That’s why it’s important to be aware of these risks and take steps to protect against them.

**REVIEW**

The growing number of cyberattacks in Nepal has become a serious issue, worrying businesses, government offices, and banks. This review looks at five major cyberattacks that have happened in Nepal in the last few years. These incidents show how vulnerable our digital systems are and why we need to take cybersecurity more seriously. By studying these cases, we can better understand the risks and learn how to protect ourselves from similar attacks in the future.

The attacks involve in the fiscal year 2020-2021, there were 3,906 reported cases of cybercrime, and in just the first three months of 2021-2022, this number reached 1,547. Nepal currently ranks 109th out of 160 countries on the National Cyber Security Index and 94th on the Global Cyber Security Index. Additionally, it ranks 140th on the ICT Development Index. These statistics highlight the growing challenges Nepal faces in cybersecurity and the urgent need for stronger measures to combat digital threats.

Another attack **Nepal’s government servers continue to face cyberattacks aimed at shutting them down**, even after hundreds of official websites were restored following a major intrusion on Saturday. The attacks disrupted services, including international travel, due to the shutdown of the immigration server. Flights were delayed, and operations were manually managed to minimize disruptions. Officials identified the attacks as **Distributed Denial of Service (DDoS)**, where multiple devices overwhelm a target with fake traffic. By Sunday, over 1,000 government websites were restored, but the main server remained under attack.

This incident highlights Nepal’s vulnerability to cyber threats. Despite improving to 94th in the Global Cybersecurity Index, Nepal’s overall score remains low at 44.99 out of 100. Experts stress the need for stronger legal frameworks, better infrastructure, and increased investment in cybersecurity. While no data was reported as compromised, concerns remain about potential breaches. Authorities are investigating the attack, but Nepal’s weak cyber infrastructure continues to pose significant risks.

In September 2020, a notable cyberattacks occurred in Nepal and targeted the Nepal Electronic Payment System which is a shared card switching facility of 17 banks. Hackers installed malware in the system which enabled them to take control of ATMs and withdraw money even before the banks received cash withdrawal requests. This case outlined the absence of adequate measures in place, especially on the side of the Nepal Rastra Bank, which shows that the country is more defenseless against such attacks.

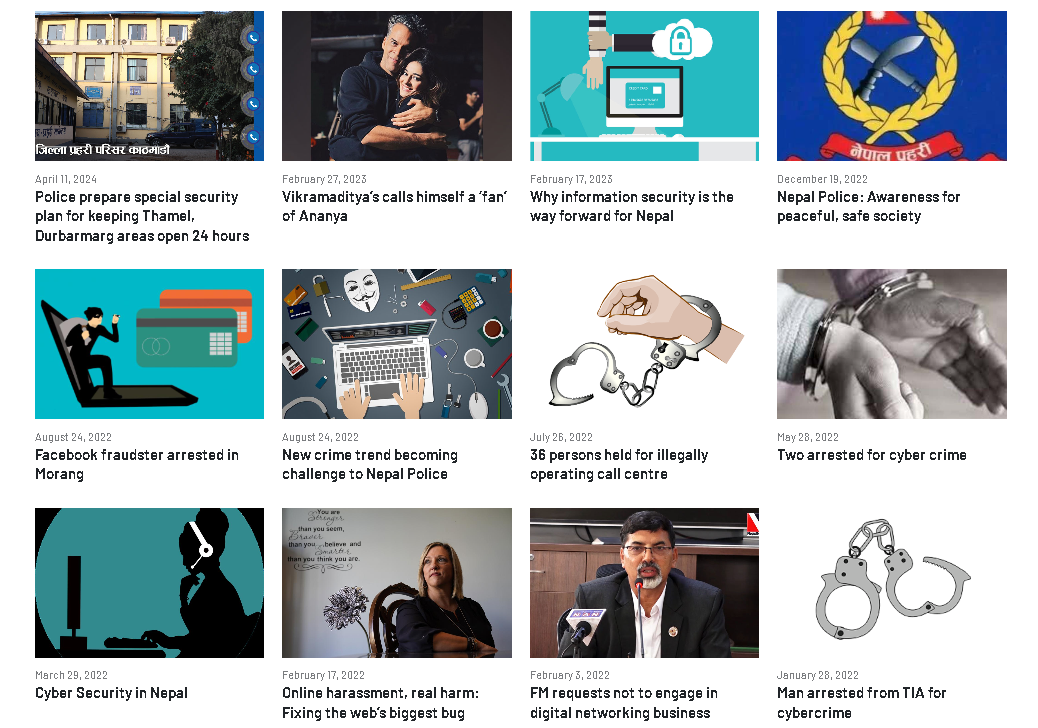
Another significant cyber-attack happened on July 25, 2017, in which the Palestinian **hacker group, Paradox Cyber Ghost hacked 58 different government servers which included the Ministry of Defense, Office of the Auditor General,** and even the Nepal Law Commission. This marked the highest portions of cyber-attacks in the government of Nepal system. Previously, in July 2015, the president of Nepal and the Department of passports official website was also hacked putting a spot light on the weak cybersecurity principles of the country. All of these examples call for more powerful measures to be in place to defend essential infrastructures.

**CYBER Incidents**

Recent cybercrime incidents in Nepal include a 2023 attack that disabled 1500 government websites, a 2021 hacking of the President's official website, and a 2017 breach that compromised over 58 government websites.

Here's a more detailed look at some notable cybercrime incidents in Nepal:

* **2023 Government Website Attack:** A cyberattack in 2023 left 1500 government websites dysfunctional.
* **2021 Presidential Website Hacking:** The official website of the President of Nepal was hacked in 2021.
* **2017 "Paradox Cyber Ghost" Breach:** A cyberattack by "Paradox Cyber Ghost" in 2017 compromised over 58 government websites.
* **2020 Nepal Electronic Payment System Attack:** Hackers injected malware into the Nepal Electronic Payment System, a shared card switching system of 17 banks, in September 2020, leading to cash withdrawals from ATMs.
* **2022 Cybercrime Cases:** In the first 3 months of the fiscal year 2021-2022, 1547 cybercrime cases were reported





**Motives of Cyber Attacks**

Cyberattacks are carried out for various reasons based on the objectives and intentions of the attacker. Knowing the motives assists in anticipating and averting cyberattacks. The following are common motives of cyberattacks:

1. Financial Gain: The majority of cyberattacks, such as ransomware or ATM hacking, are motivated by financial reasons. Hackers target banks, businesses, and individuals with the aim of stealing money or demanding ransoms.

2. Political or Ideological Motives: Some attacks are carried out to spread political messages, protest against governments, or promote particular ideologies. For instance, hacking government websites to leave political messages.

3. Espionage: Cyberattacks are generally utilized to steal sensitive data, such as government secrets, corporate data, or personal data, for strategic or competitive advantages.

4. Disruption of Services: Hackers may attack critical services such as transportation, healthcare, or communications to create havoc or to prove a point.

5. Revenge or Personal Grudges: Hackers sometimes attack systems to fulfill personal vendettas or seek revenge against organizations or individuals.

6. Testing Skills or Fun: Some hackers, especially amateurs, carry out attacks just to test their skills or for fun, without considering the consequences.

7. Terrorism: Cyberattacks can be used as a tool by terrorist groups to compromise national security or cause widespread fear.

Considering these motivations, governments, businesses, and individuals can better prepare and defend themselves against potential cyber-attacks.

**THE PREVENTIVE MEASURES**

Preventive measures are steps taken to reduce the risk of harm or threats. In cybersecurity, these are actions that individuals and organizations can take to lower the chances of cyberattacks and lessen their impact. Here are some common preventive measures:

**Steps to Implement Before an Attack:**

1. Risk Assessments and Threat Modeling:

- Conduct regular vulnerability assessments.

- Perform threat modeling to identify potential attack vectors and prioritize defenses.

2. Strong Access Controls:

- Enforce multi-factor authentication (MFA) for all users.

- Implement role-based access control (RBAC) to limit access to sensitive systems and data.

3. Regular Security Assessments:

- Conduct penetration testing to simulate real-world attacks.

- Identify and address vulnerabilities proactively.

4. Data Encryption:

- Encrypt data both at rest and in transit using strong protocols (e.g., AES-256, TLS 1.3).

5. Employee Cybersecurity Training:

- Train employees on cybersecurity best practices, including phishing and social engineering awareness.

- Conduct regular security awareness campaigns.

6. Incident Response Planning:

- Develop and maintain a robust incident response plan.

- Conduct regular drills to ensure preparedness.

7. Patch Management:

- Regularly update and patch software, operating systems, and firmware.

- Monitor vendor updates and apply them promptly.

8. Network Segmentation:

- Divide networks into segments to limit attacker movement.

- Use firewalls and intrusion detection/prevention systems (IDS/IPS) to block malicious traffic.

9. Third-Party Security Evaluation:

- Assess the security of third-party vendors and partners.

- Ensure third-party systems integrated with NEPS are secure.

10. Data Backup and Recovery:

- Maintain regular backups of critical data.

- Test disaster recovery plans to ensure quick restoration.

**Future Measures to Prevent Similar Attacks:**

1. Adopt Zero Trust Architecture:

- Trust no user or device by default; verify all access requests.

- Continuously monitor and validate user activity.

2. Advanced Threat Detection and Monitoring:

- Use Security Information and Event Management (SIEM) solutions for real-time monitoring.

- Leverage AI and machine learning to detect anomalies and threats.

3. Enhanced Endpoint Security:

- Deploy Endpoint Detection and Response (EDR) solutions on all devices.

- Regularly scan endpoints for malware and vulnerabilities.

4. Collaboration with Cybersecurity Agencies:

- Partner with national and international cybersecurity organizations.

- Participate in information-sharing initiatives to stay updated on emerging threats.

5. Regular Red Team Exercises:

- Conduct red teaming to test the effectiveness of defenses.

- Use findings to improve security measures.

6. Implement Blockchain for Transaction Security:

- Explore blockchain technology to secure financial transactions and ensure tamper-proof records.

7. Continuous Improvement of Security Policies:

- Regularly review and update security policies.

- Align with global standards like ISO 27001, PCI DSS, and NIST.

8. Public-Private Partnerships:

- Collaborate with financial institutions and cybersecurity firms to strengthen defenses.

9. User Education and Phishing Simulations:

- Continuously educate users on cybersecurity risks.

- Conduct phishing simulations to test and improve employee awareness.

10. Invest in Cybersecurity Talent and Tools:

- Hire skilled cybersecurity professionals.

- Invest in advanced security tools and technologies.

11. Regulatory Compliance and Audits:

- Adhere to local and international cybersecurity regulations.

- Conduct regular external audits to validate security measures.

12. Public Awareness Campaigns:

- Educate the public on safe online practices to reduce the risk of account compromises.

By implementing these measures, organizations can significantly reduce the risk of cyberattacks and ensure the resilience of critical financial infrastructure.

&

By these measures, the Nepal Electronic Payment System and similar other important financial infrastructures can significantly reduce the likelihood of falling prey to cyberattacks and enhance their security profile overall.

**INCIDENT RESPONSE**

Incident response, or cybersecurity incident response, is the technology and process by which an organization detects and responds to cyber threats, security incidents, or cyberattacks. Its main goals are to proactively block cyberattacks before they happen and to reduce the cost and disruption of any attack that does get through.

**Some of the most common types of security incidents include:**

- Ransomware: Software that encrypts the data or device of a victim and demands a ransom. Ransomware attacks increased by 41% between 2021 and 2022.

- Phishing Attacks: Use emails, messages, or calls to trick people into revealing sensitive information or executing malicious actions. Phishing is the costliest and second most common reason for data breaches, as well as the most common type of social engineering.

- DDoS Attacks: These overwhelm a target's servers or network with traffic, making them unavailable to legitimate users.

- Supply Chain Attacks: These infiltrate an organization through its suppliers or use their services to spread malware.

- Insider Threats: These occur due to authorized users who, knowingly or unknowingly, compromise security by not following best practices.

Through an efficient incident response plan, organizations can protect themselves from such threats and minimize the impact of cyberattacks.

**RELATED SOLUTIONS**

IBM Security has numerous tools and services that can help organizations stay safe from cyber threats and handle attacks better. Some of their solutions are mentioned below:

1. X-Force Incident Response Team:

- This is a team of expert cybersecurity professionals who help organizations respond to cyberattacks quickly. They work to reduce the damage caused by the attack and help the organization recover faster.

2. Security Orchestration, Automation, and Response (SOAR):

- It helps in speeding up the reaction to cyber incidents using automation. It also automates operations and connects with other security products to make sure that everything operates at its best.

3. Managed Detection and Response Services:

- This service offers 24/7 cyber protection. It leverages intelligent technology and expert professionals to identify and block sophisticated threats before they harm the system.

These solutions enable organizations to remain ready and secure against cyberattacks, facilitating easy management of any issues that arise their way.

**CONCLUSION**

In general, Nepal is increasingly vulnerable to cyberattacks, as seen in recent incidents like the hacking of government websites, financial systems, and even the official website of the President. Some of these are the 2023 hack of 1,500 government websites and the 2020 hacking of the Nepal Electronic Payment System, which demonstrate the vulnerabilities in the country's cybersecurity system. With over 3,900 instances of cybercrime reported for 2020-2021 and 1,547 for just the first quarter of 2021-2022, it is clear that Nepal is getting increasingly vulnerable. While there is improvement visible, such as ranking 94th in the Global Cybersecurity Index, Nepal's overall score remains low, and the country performs poorly in ICT development.

This calls for a need in the immediate present for stronger cybersecurity, including enhanced infrastructure, stringent legislation, and increased investment in cyber security. Through learning the lessons of history and being preventive, Nepal is better placed to safeguard its firms, government systems, and populace from future cyber-attacks. Cooperation, training, and awareness form the cornerstones of developing a safer digital sphere for the country.

**References**

1. Introduction and Overview of Cyberattacks in Nepal:

- The article presents an overview of cybersecurity and cyberattacks and addresses recent trends within Nepal, including hacking on government websites and financial networks. It identifies the heightened potential for cyberattacks with heightened movement of services into the digital medium and places greater focus on raising awareness and initiating preventive measures.

2. Statistics and Rankings:

- Figures of cybercrime incidents in Nepal, e.g., 3,906 in 2020-2021 and 1,547 in the first quarter of 2021-2022, are given. Positions of Nepal on the National Cyber Security Index (109th), Global Cybersecurity Index (94th), and ICT Development Index (140th) are stated to reflect the cybersecurity challenges of the country.

3. Notable Cyber Incidents:

- Some incidents, such as the 2023 hacking of 1,500 government websites, the 2021 hacking of the President's official website, the 2017 "Paradox Cyber Ghost" breach of 58 government websites, and the 2020 Nepal Electronic Payment System attack, are described to identify Nepal's vulnerabilities.

4. Motives for Cyberattacks:

- The usual motives behind cyberattacks, which are **financial gain, political or ideological motives, espionage, disruption of services, revenge, testing of capability, and terrorism,** are elaborated in the article.

5. Preventive Measures:

- Preventive measures against cyberattacks are suggested, including **training staff, updating software, endpoint security, firewalls, data backup, access control, and use of secure passwords.**

6. Incident Response:

- Incident response plans are emphasized to be critical, with examples of common security incidents **like ransomware, phishing, DDoS attacks, supply chain attacks, and insider threats.**

7. Related Solutions:

- IBM Security's solutions like the **X-Force Incident Response Team, Security Orchestration, Automation, and Response** **(SOAR), and Managed Detection and Response Services** are emphasized as solutions to improve cybersecurity.

8. Conclusion:

- The conclusion emphasizes the increasing susceptibility of Nepal to cyberattacks and calls for more effective cybersecurity, including stronger infrastructure, tougher legislation, and greater investment. It focuses on learning from history and fostering awareness, training, and collaboration for the sake of making a safer digital future.

This article condenses information from a variety of cyber breaches, statistical data, and expert recommendations to show a complete picture of Nepal's cybersecurity problem and resolution.

Source: <https://nepalnews.com/tag/cyber-crime/page/2/>

<https://aag-it.com/the-latest-cyber-crime-statistics/>

<https://kathmandupost.com/national/2023/01/30/singha-durbar-server-continues-to-face-cyberattacks>

<https://gtn.com.np/2023/02/cyberattacks-in-nepal/>

<https://nepalindata.com/ne/Four-Nepal-Government-Websites-Hacked-with-Critical-Information-dumped-by-malicious-actors/>

And getting help from CHATGPT too.

To From

Badri Tamang Hiran Rajbanshi