Network Security Issues in Modern Infrastructure

(NSP-Sec, DDoS, Anti-Spam, and Anti-Malware)

#ABOUT ME#

Er. Jeet Narayan Yadav

- **Education**: Master's in Computer Engineering (M.E.)
- **Rank** : Deputy Superintendent of Police (DySP)
- **Role** System & Security Engineer
- **Organization**: Nepal Police, IT Directorate, PHQ, Naxal
- Email Address: jeet@nepalpolice.gov.np
- Mobile No: +977-9851051877
- **Professional Experience**: Over 22 years of expertise in the IT sector, specializing in system and security while leading the Security and System Team at Nepal Police.

ῷ **Achievements :Professional Certifications**

- MCSE Windows NT 4.0,
- CCNA ,
- Certified SOC Analyst (CSA), Fortinate **NSE 4.0**

ῷ **Academic Contributions**: Actively associated with academia to share expertise & foster learning.

ῷ **Professional Goals :** Continue enhancing **leadership skills** and **technical expertise**. Implement **advanced security measures** to protect Nepal Police's digital assets.

Outline

Advanced Security Threats in holistic system

Security Challenges

Discuss some Use cases of Cyber crime in Nepal

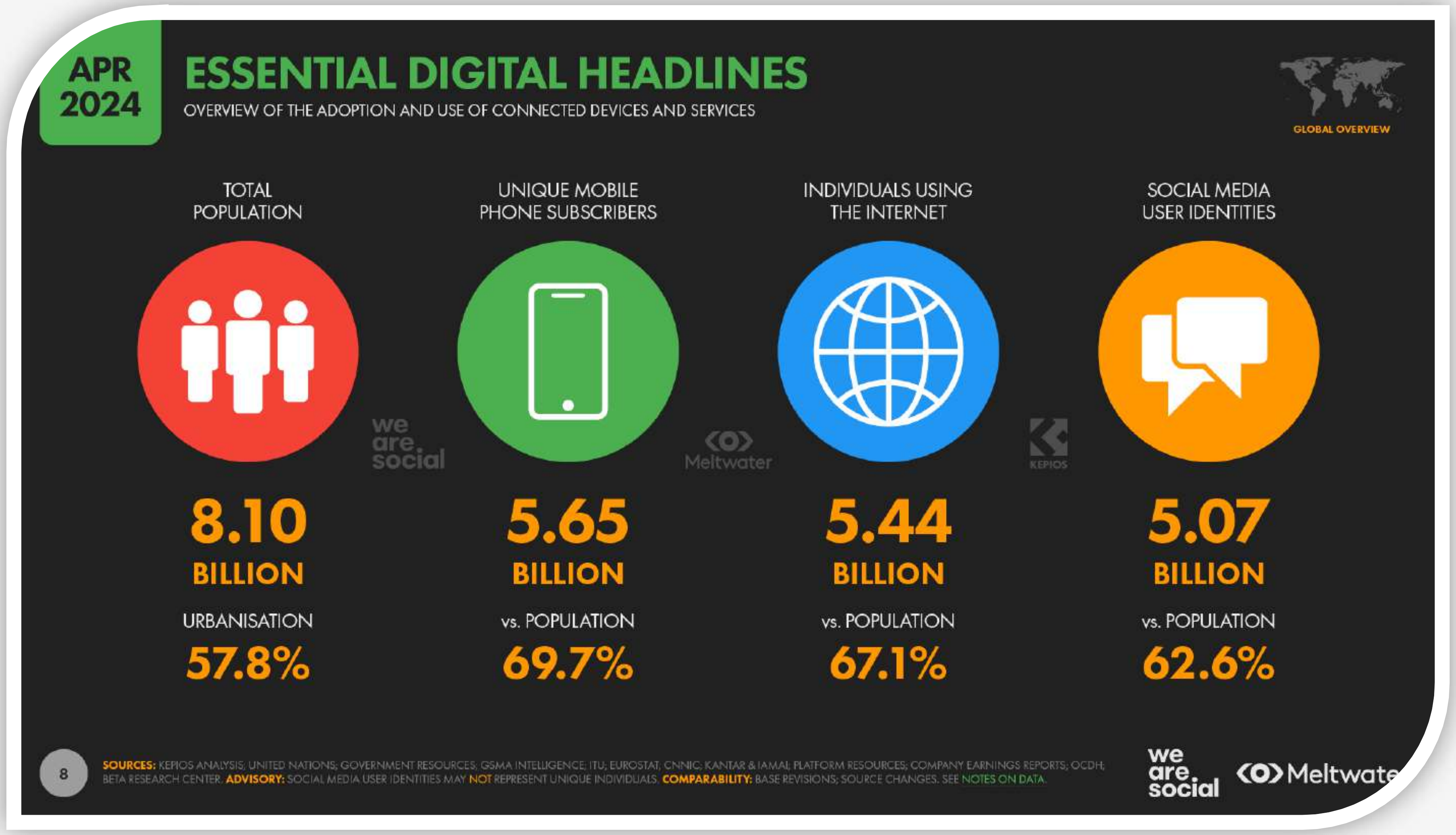
Security Recommendation

Security Quote

“ Security is not a product, but a process.
Trust, but verify.“

- Bruce Schneier *A Security Expert*

The complete Global Digital 2024 Report



APR 2024

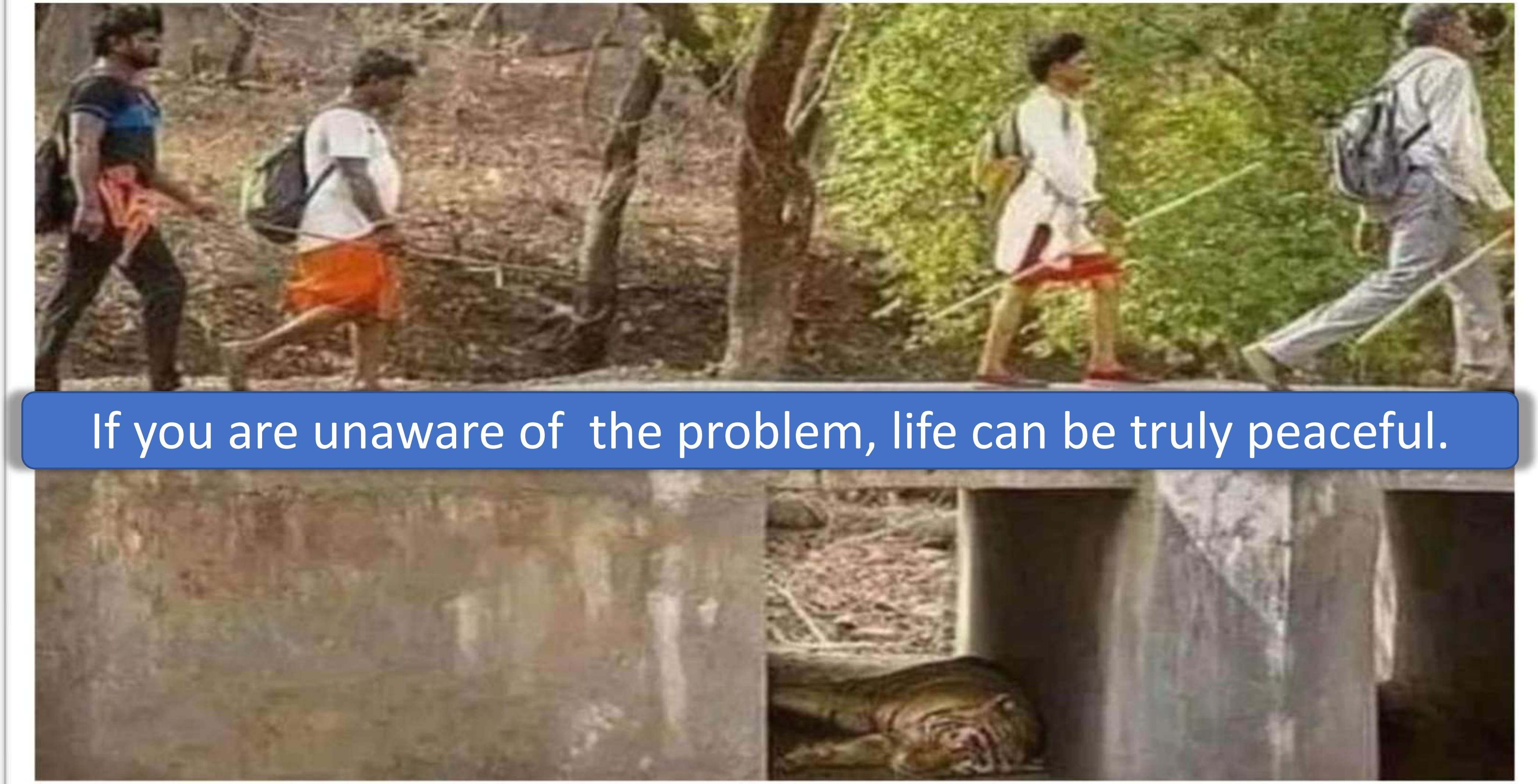
ESSENTIAL DIGITAL HEADLINES

OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES

TOTAL POPULATION	UNIQUE MOBILE PHONE SUBSCRIBERS	INDIVIDUALS USING THE INTERNET	SOCIAL MEDIA USER IDENTITIES
8.10 BILLION	5.65 BILLION	5.44 BILLION	5.07 BILLION
URBANISATION	vs. POPULATION	vs. POPULATION	vs. POPULATION
57.8%	69.7%	67.1%	62.6%

SOURCES: KEPIOS ANALYSIS; UNITED NATIONS; GOVERNMENT RESOURCES; GSMA INTELLIGENCE; ITU; EUROSTAT; CNNIC; KANTAR & IAMAI; PLATFORM RESOURCES; COMPANY EARNINGS REPORTS; OCDH; BETA RESEARCH CENTER. ADVISORY: SOCIAL MEDIA USER IDENTITIES MAY NOT REPRESENT UNIQUE INDIVIDUALS. COMPARABILITY: BASE REVISIONS; SOURCE CHANGES. SEE NOTES ON DATA.

Digital 2024 April Global Statshot Report — DataReportal – Global Digital Insights



If you are unaware of the problem, life can be truly peaceful.

Advanced Security Threats in Holistic system

Advanced Security threats in Holistic system

- Advanced security threats are cyberattacks that are designed to be difficult to detect, and often use a combination of attack methods. Some common advanced security threats include:
  - Advanced persistent threat (APT)
  - DNS attack
  - Malware
  - Phishing
  - DDoS attacks
  - Spam
  - Ransomware
  - Social engineering
  - **Insider threats** Etc.

Network Security tools designed to protect users and systems from various digital threats.

Some of Advanced Security Solutions

Anti-Spam

NextGen Firewall

Anti Phishing

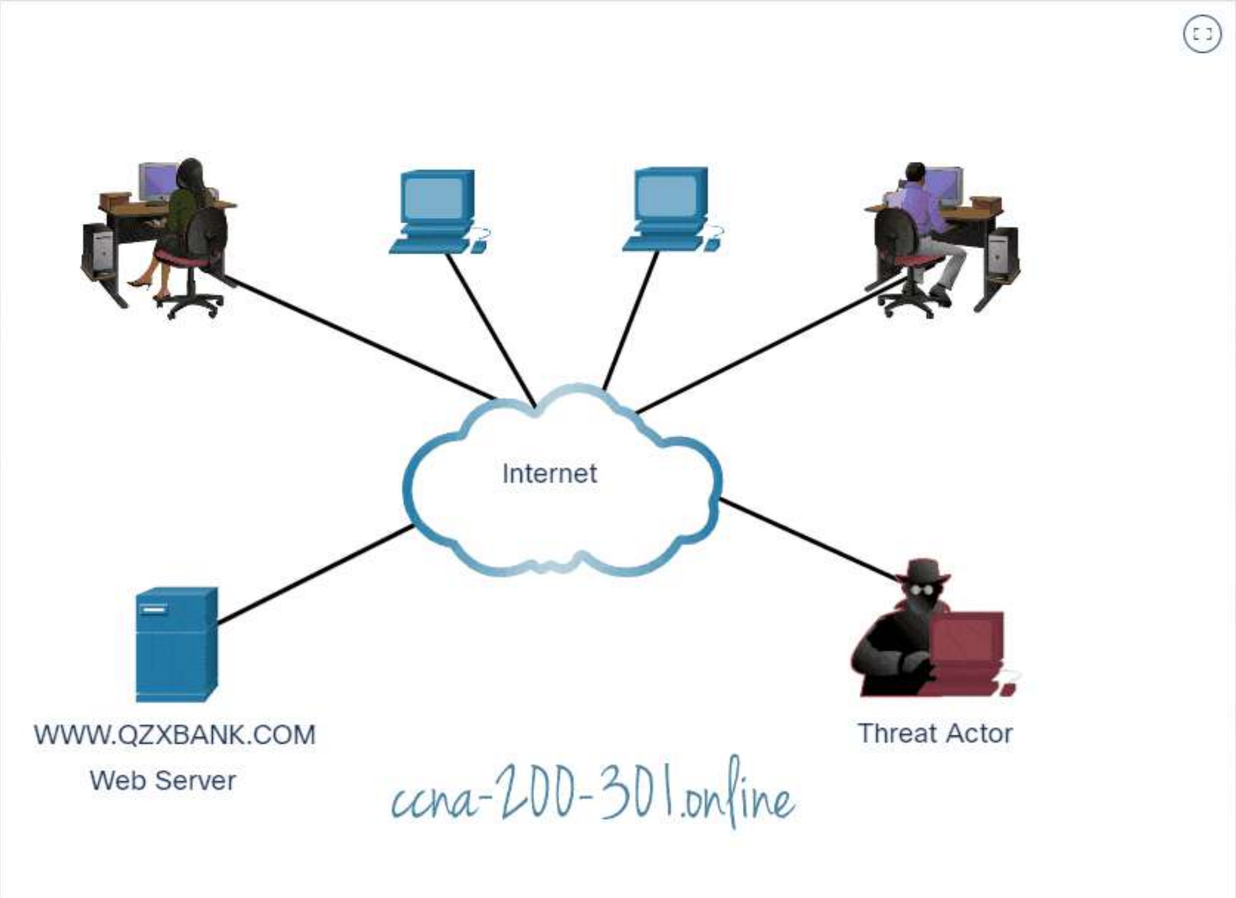
NSP-Sec :
Network Security
Protocol Security

Anti-Malware

DDoS control

DDoS and Spam Attacks

DDoS and Spam attacks



DDoS attack

Spam attack

DDoS Attacks: Distributed Denial of Service attacks

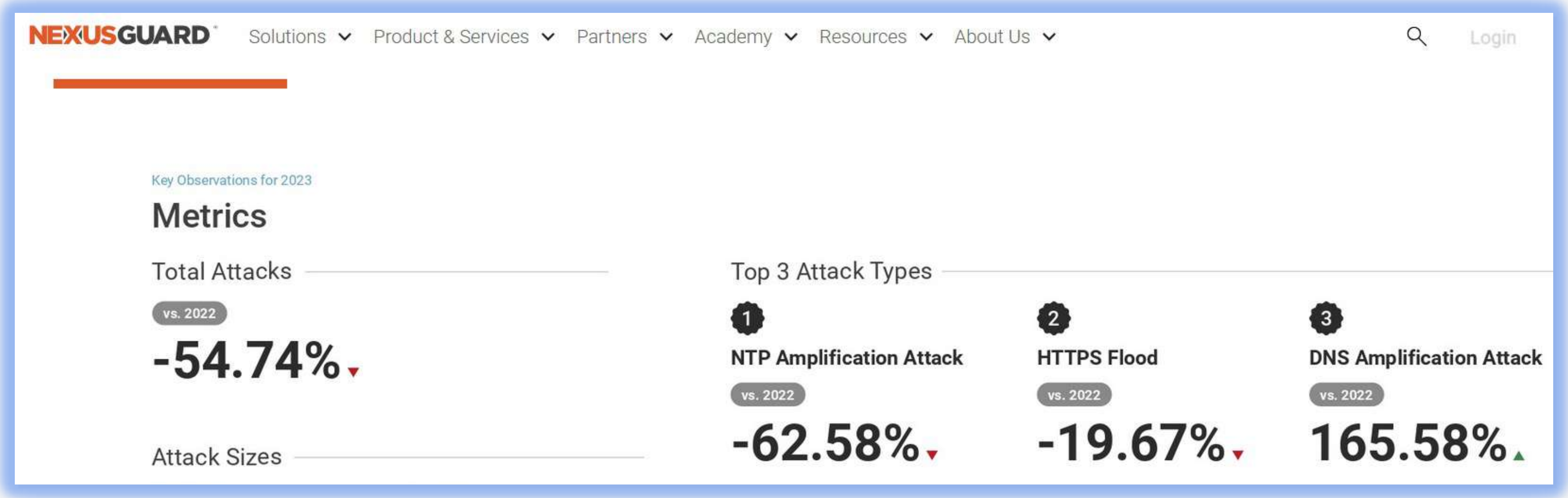
Common Types of DDoS Attacks

- ❑ **Volume-Based Attacks:** Overload bandwidth (e.g., UDP floods, ICMP floods).

- ❑ **Protocol Attacks:** Exploit vulnerabilities in protocols (e.g., SYN flood, Ping of Death).

- ❑ **Application-Layer Attacks:** Target specific applications (e.g., HTTP flood, Slowloris).

DDoS Attacks: Report



Key Observations for 2023

Metrics

Total Attacks

vs. 2022

-54.74%▼

Attack Sizes

Top 3 Attack Types

1 NTP Amplification Attack

vs. 2022

-62.58%▼

2 HTTPS Flood

vs. 2022

-19.67%▼

3 DNS Amplification Attack

vs. 2022

165.58%▲

https://www.nexusguard.com/threat-report/ddos-trend-report-2024#download-report

Anti-Spam

Anti-Spam

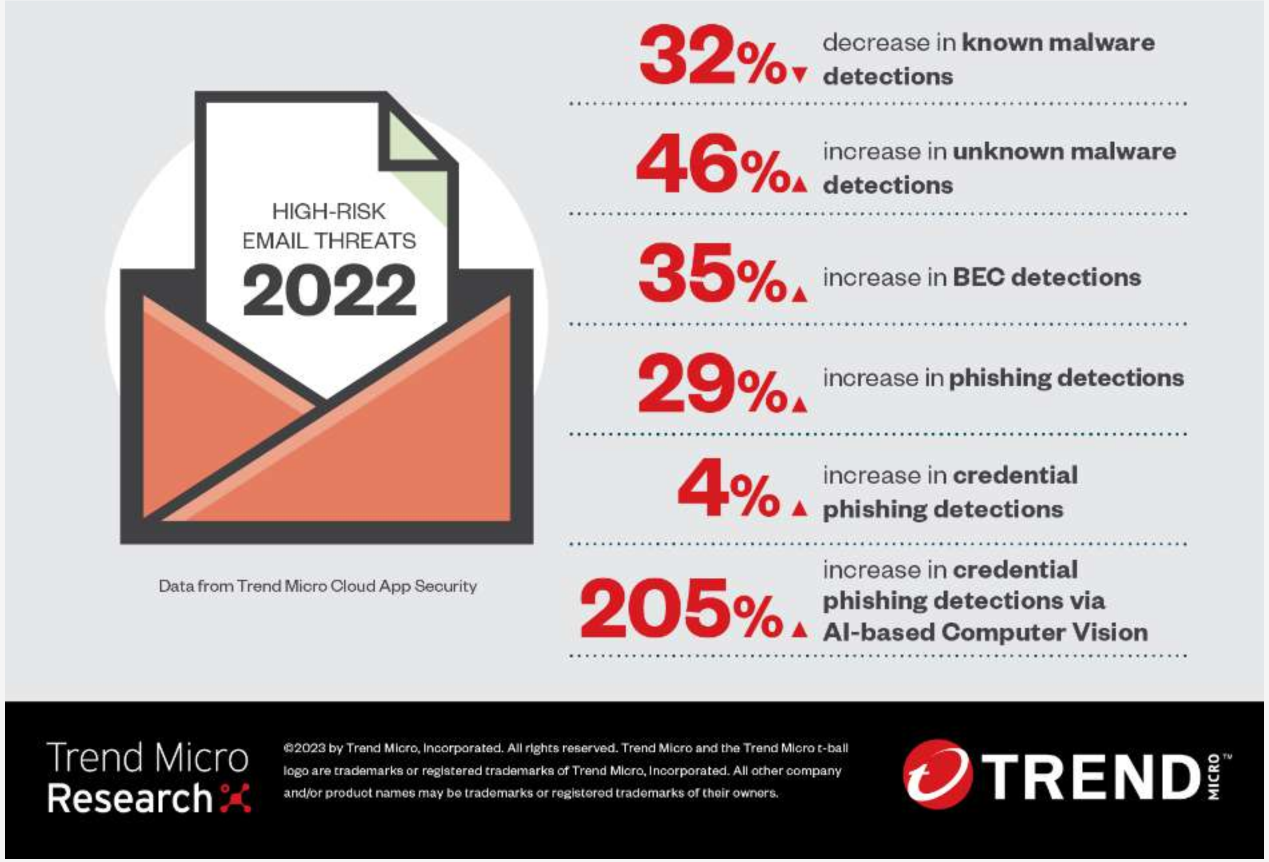
- ❑ **Anti-spam** refers to techniques and tools designed to detect, filter, and block unwanted, unsolicited, or malicious emails and messages, commonly known as spam. Spam often clutters inboxes, poses security risks, and consumes valuable network resources.

Anti-Spam

Common Tools and Technologies

- ❑ **Email Gateways :** Tools like Proofpoint, Mimecast, or Barracuda for enterprise-level email security.
- ❑ **Spam Filters :** Built into email services (e.g., Gmail, Outlook) or third-party tools like SpamAssassin.
- ❑ **DNSBL Services :** Services like Spamhaus or SURBL to block known spam sources.

Anti-Spam



HIGH-RISK EMAIL THREATS 2022

32%▼ decrease in **known malware detections**

46%▲ increase in **unknown malware detections**

35%▲ increase in **BEC detections**

29%▲ increase in **phishing detections**

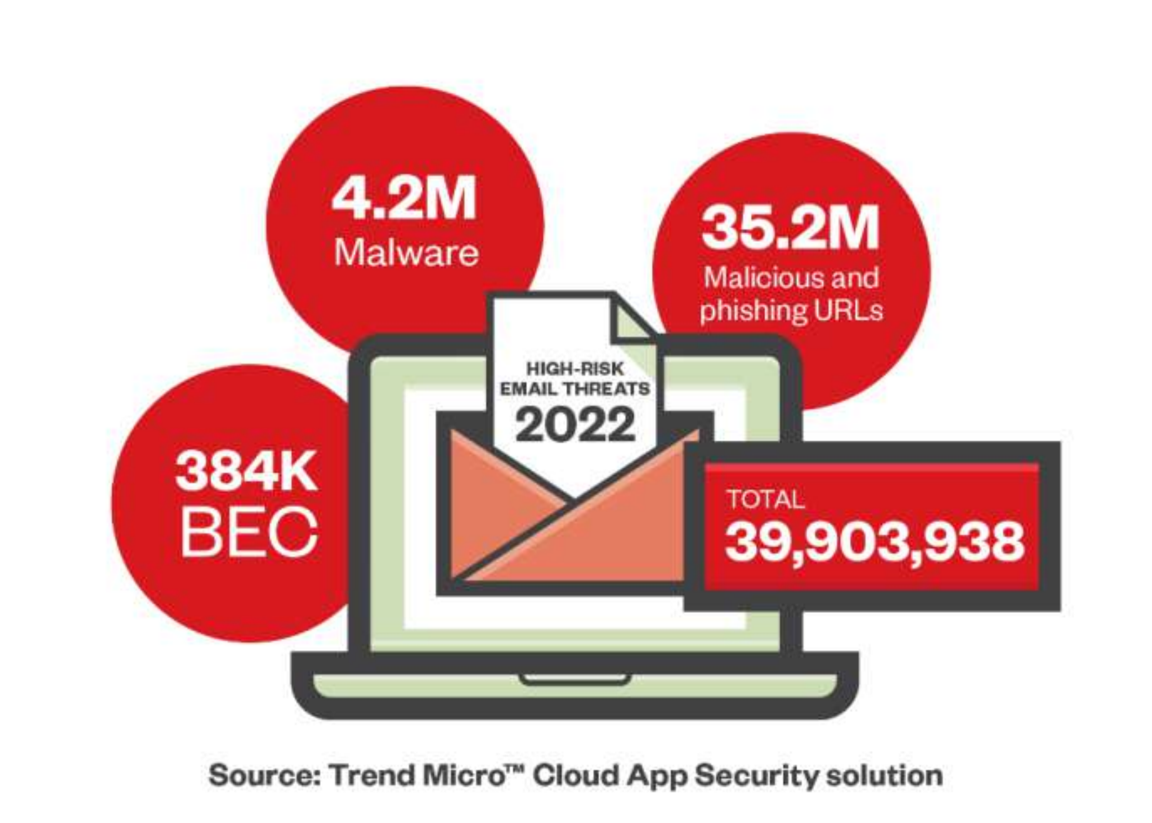
4%▲ increase in **credential phishing detections**

205%▲ increase in **credential phishing detections via AI-based Computer Vision**

Data from Trend Micro Cloud App Security

Trend Micro Research

TREND MICRO™



Source: Trend Micro™ Cloud App Security solution

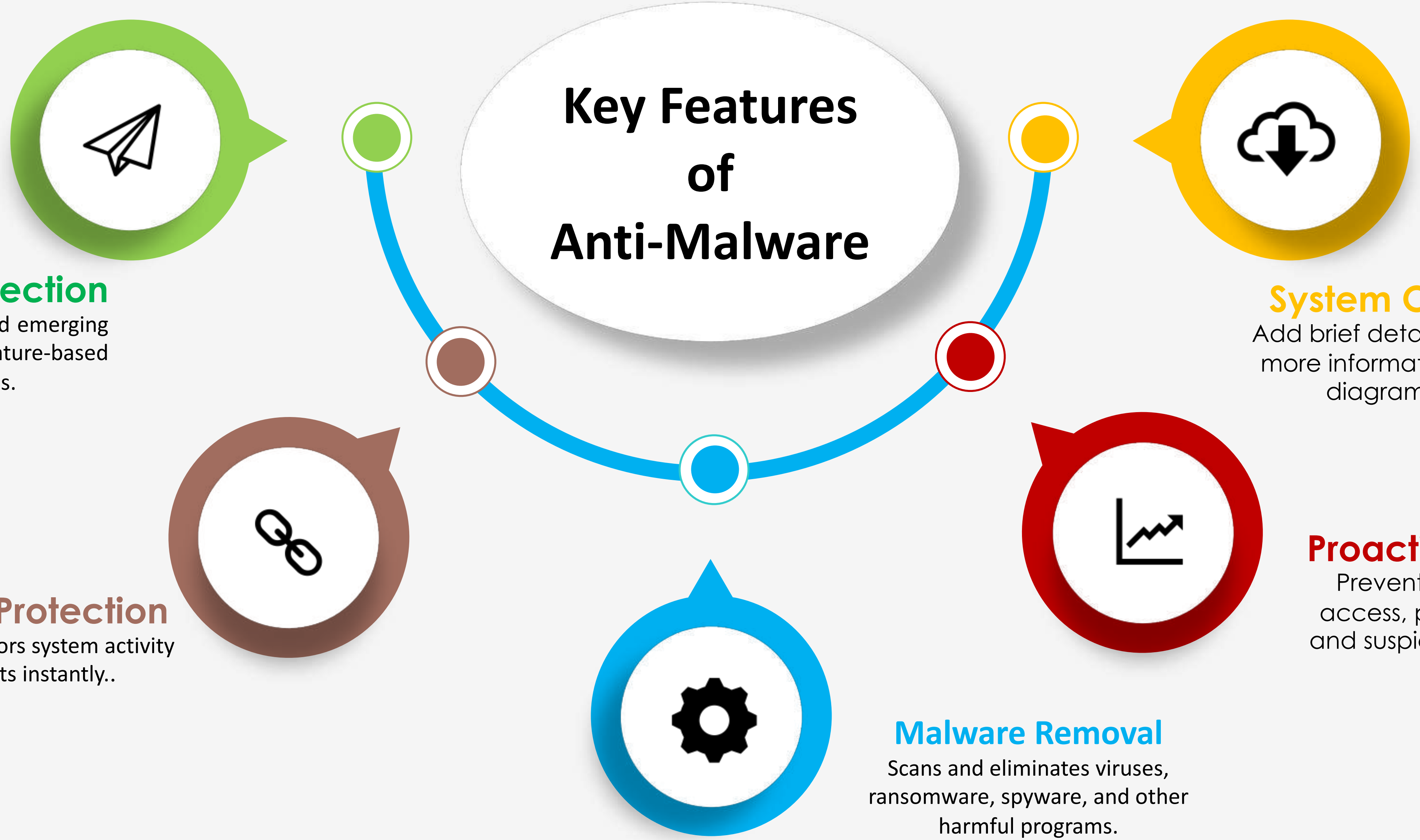
Source: https://documents.trendmicro.com/images/TEx/articles/cas-threat-report-2022-InfogBVksMXV.png

Anti-Malware

Anti-Malware

- Anti-malware is **Intelligent Software** designed to protect computer systems, networks, and devices by ***detecting, blocking, and removing harmful threats*** collectively known as malware.
- This includes a wide range of threats such as ***viruses, worms, ransomware, spyware, adware, trojans,*** and more, ensuring a secure and seamless digital environment.

Anti-Malware :



Key Features of Anti-Malware

Threat Detection

Identifies known and emerging malware using signature-based and heuristic analysis.

Real-Time Protection

Continuously monitors system activity to block threats instantly..

Malware Removal

Scans and eliminates viruses, ransomware, spyware, and other harmful programs.

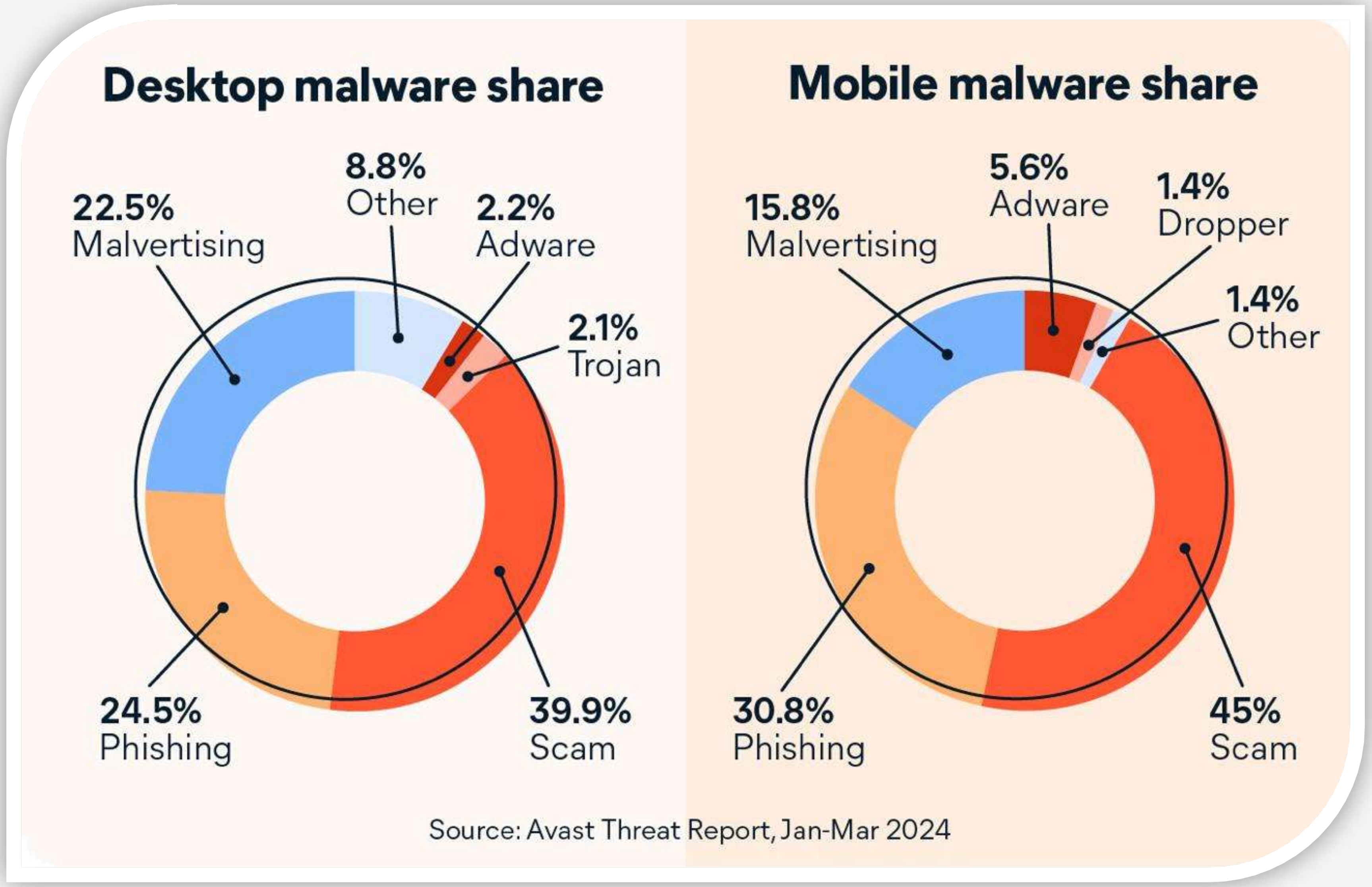
Proactive Defense

Prevents unauthorized access, phishing attacks, and suspicious downloads.

System Optimization

Add brief details here to give you more information about the bar diagram parameter.

Malware Statistic



Source: Avast Threat Report, Jan-Mar 2024

Some Use cases of Cyber crimes in Nepal

Use Case Discussions

Cyber security Incidents in Nepal

❑ It is said that **cybercrime** came into the spotlight in **2013**. Even though the exact first cyber incident of Nepal is unknown, here are some of the early crimes that took place in Nepal:

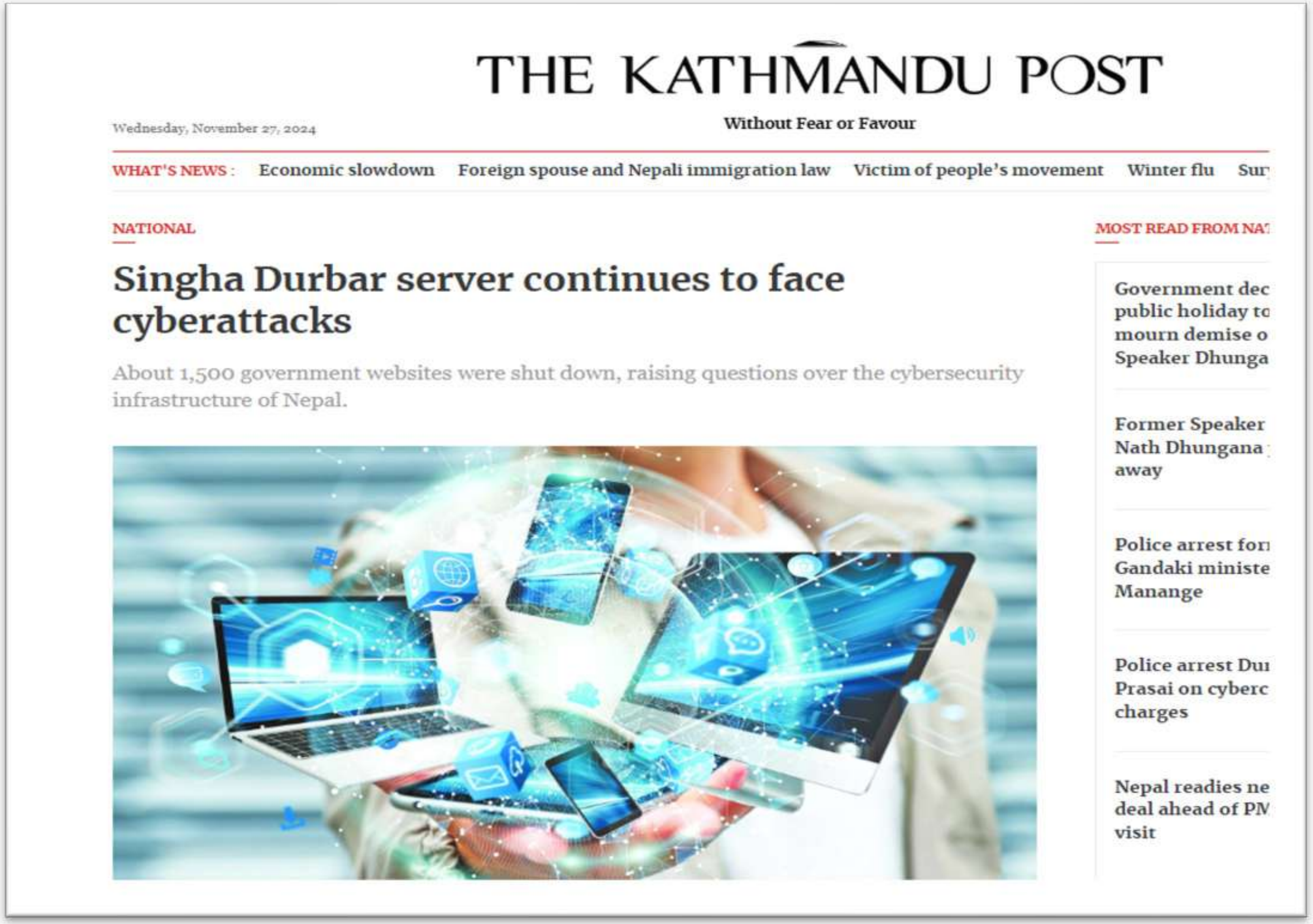
❑ **In July 2013**, a young woman fell victim to **online swindling**. She transferred **Rs. 110,000** for an online air booking. She got back only Rs. 15,000.

.

Use Case Discussions : Cyber Security incidents in Nepal

- ❑ **DDoS Attack:** Distributed Denial-of-Service (DDoS) attack targeted the GIDC system (January 30, 2023).

Use Case Discussions : Cyber Security incidents in Nepal



THE KATHMANDU POST

Wednesday, November 27, 2024

Without Fear or Favour

WHAT'S NEWS : Economic slowdown Foreign spouse and Nepali immigration law Victim of people's movement Winter flu Sur

NATIONAL

Singha Durbar server continues to face cyberattacks

About 1,500 government websites were shut down, raising questions over the cybersecurity infrastructure of Nepal.

MOST READ FROM NAT

Government dec public holiday to mourn demise o Speaker Dhunga

Former Speaker Nath Dhungana away

Police arrest for Gandaki ministe Manange

Police arrest Du Prasai on cyberc charges

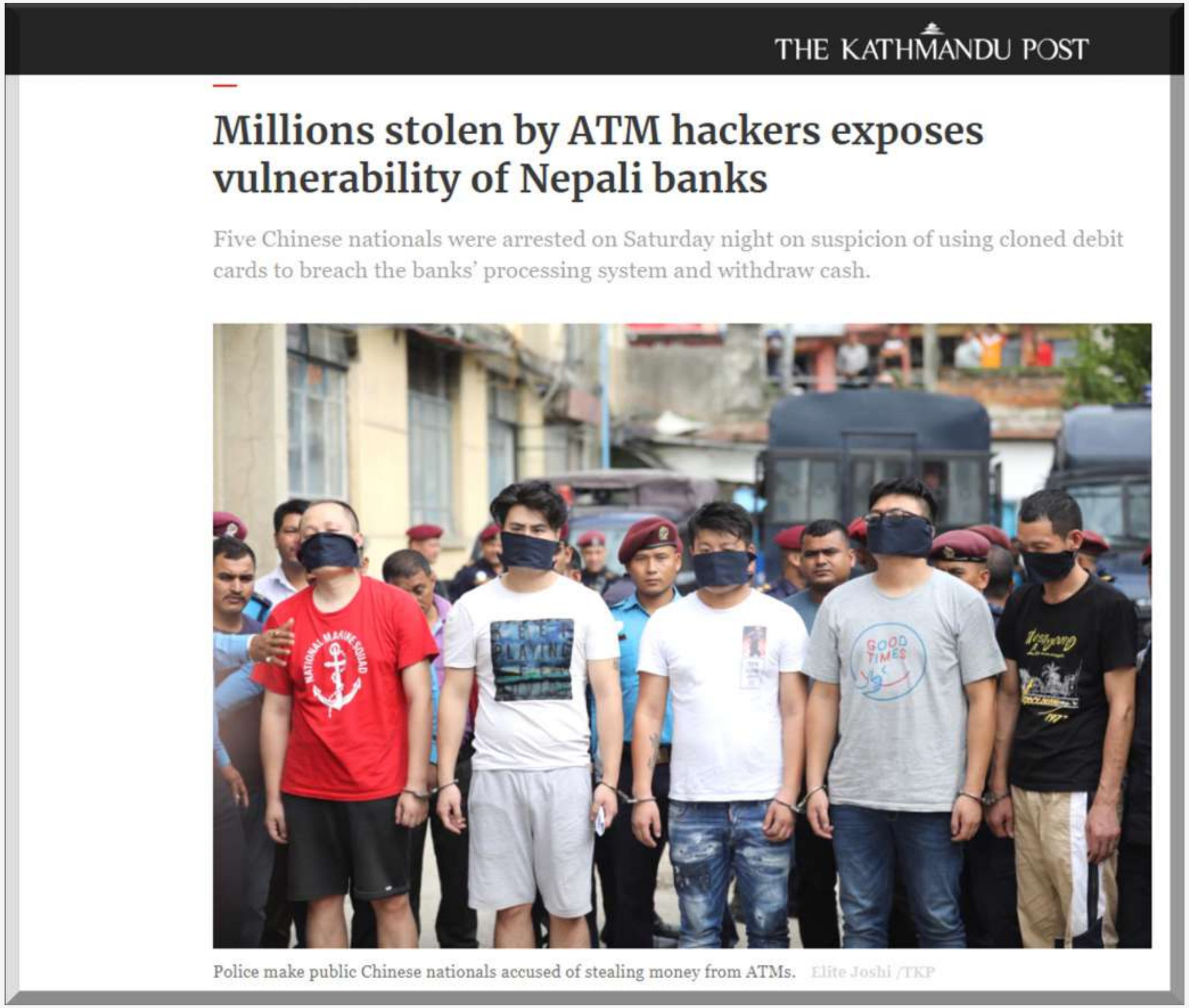
Nepal readies ne deal ahead of PM visit

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

Use Case Discussions : Cyber Security incidents in Nepal

❑ **ATM Fraud:** Chinese nationals withdrew large sums of money from ATMs (NEPS- **Nepal Electronic Payment Systems** breach, **2019**).

Use Case Discussions : Cyber Security incidents in Nepal



THE KATHMANDU POST

Millions stolen by ATM hackers exposes vulnerability of Nepali banks

Five Chinese nationals were arrested on Saturday night on suspicion of using cloned debit cards to breach the banks' processing system and withdraw cash.

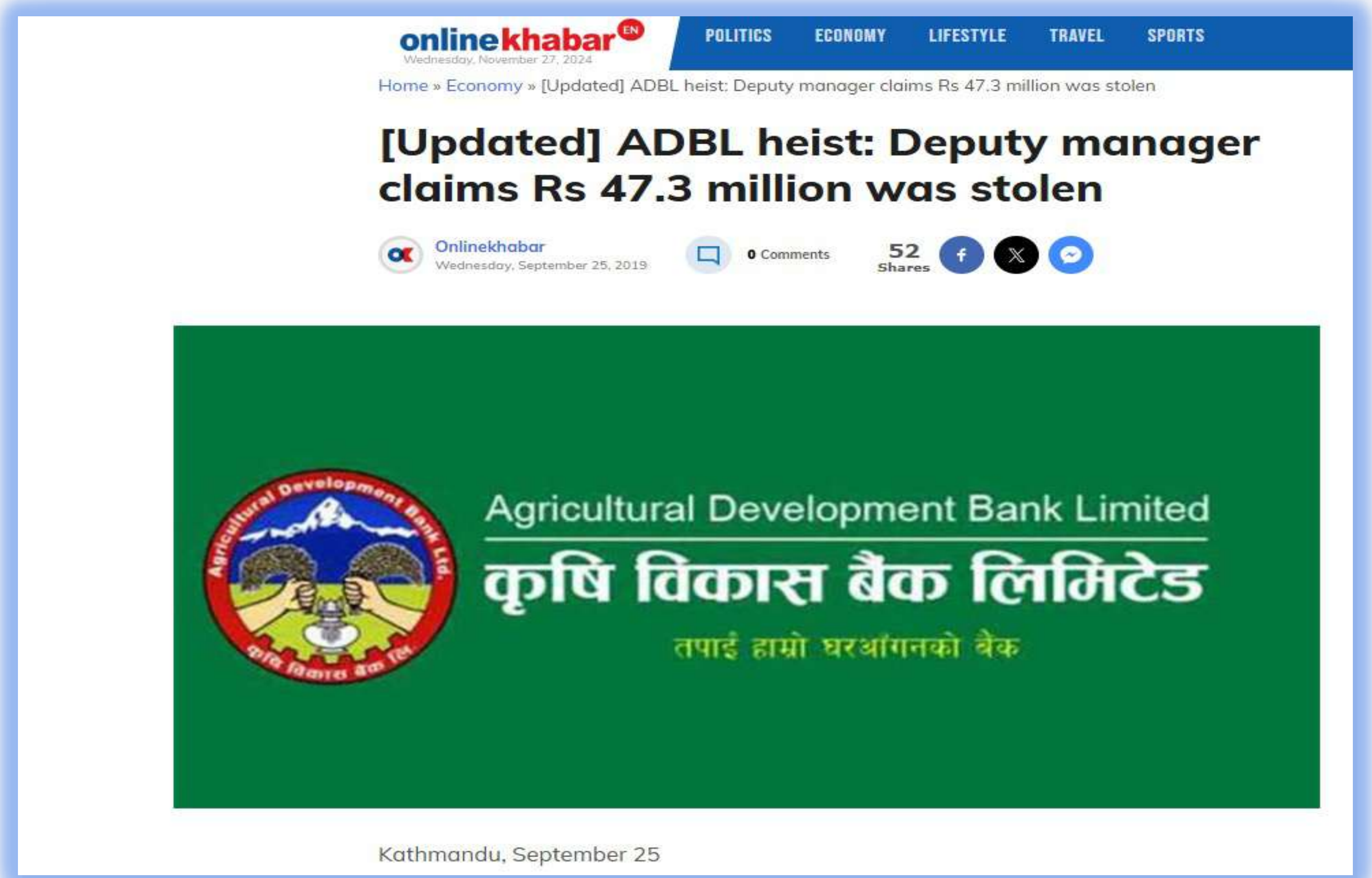
Police make public Chinese nationals accused of stealing money from ATMs. Elite Joshi /TKP

Use Case Discussions : Cyber Security incidents in Nepal

Cyber security Incidents in Nepal

❑ **Malware Attack:** Huge amounts of money stolen via malware at ADBL (2019).

State of cyber security space



onlinekhabar EN
Wednesday, November 27, 2024

POLITICS ECONOMY LIFESTYLE TRAVEL SPORTS

Home » Economy » [Updated] ADBL heist: Deputy manager claims Rs 47.3 million was stolen

[Updated] ADBL heist: Deputy manager claims Rs 47.3 million was stolen

Onlinekhabar
Wednesday, September 25, 2019

0 Comments

52 Shares

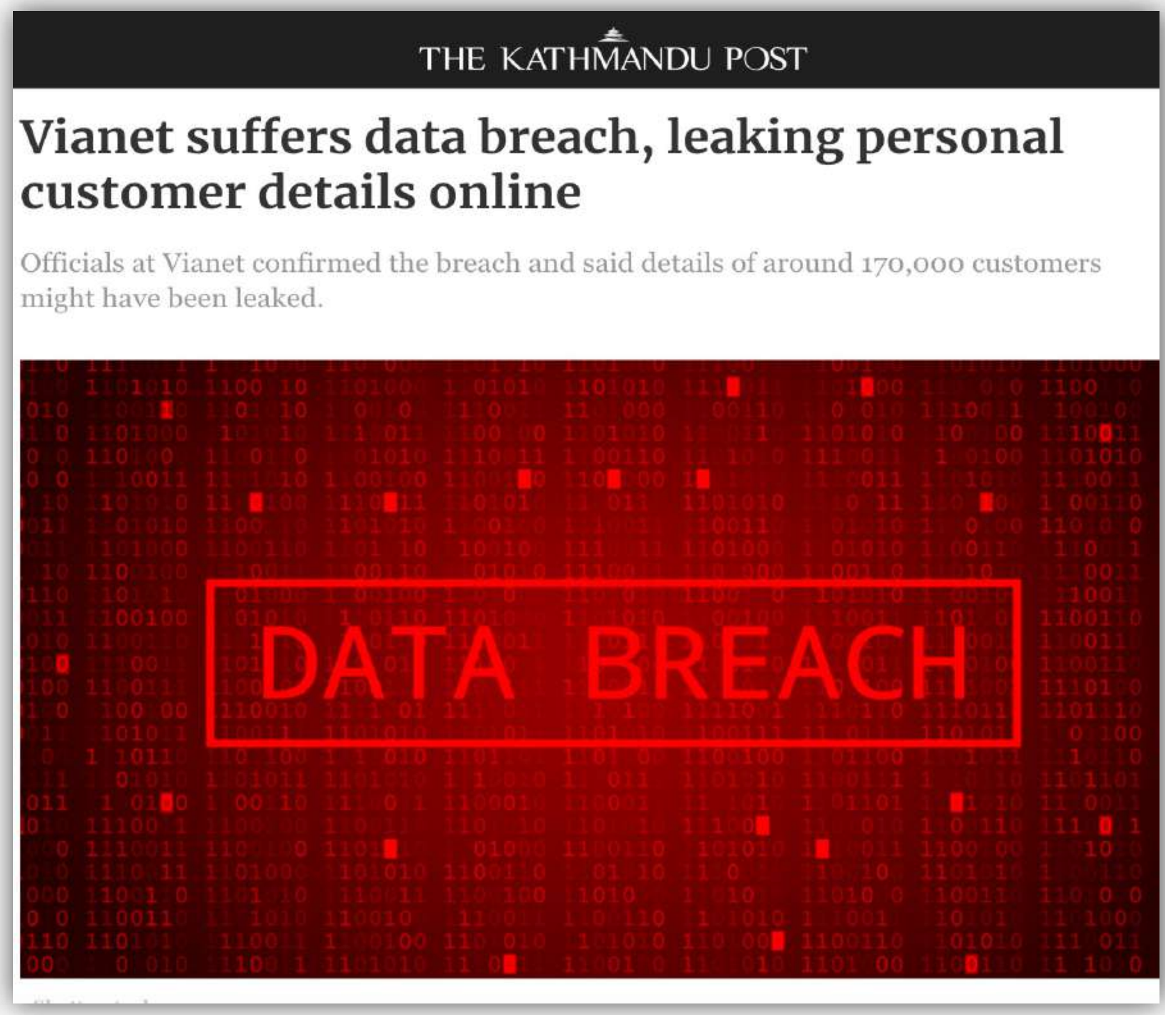
Agricultural Development Bank Limited
कृषि विकास बैंक लिमिटेड
तपाईं हाम्रो घरआँगनको बैंक
Agricultural Development Bank Ltd.
कृषि विकास बैंक लि

Kathmandu, September 25

Use Case Discussions : Cyber Security incidents in Nepal

- ❑ **Website Hacking:** Multiple websites were compromised.
- ❑ **Narpichas @paapi_kto_mah**, Twitter handler leaked the customer data of more than **160,000** customers of ***Vianet Communication on April 8, 2020,***

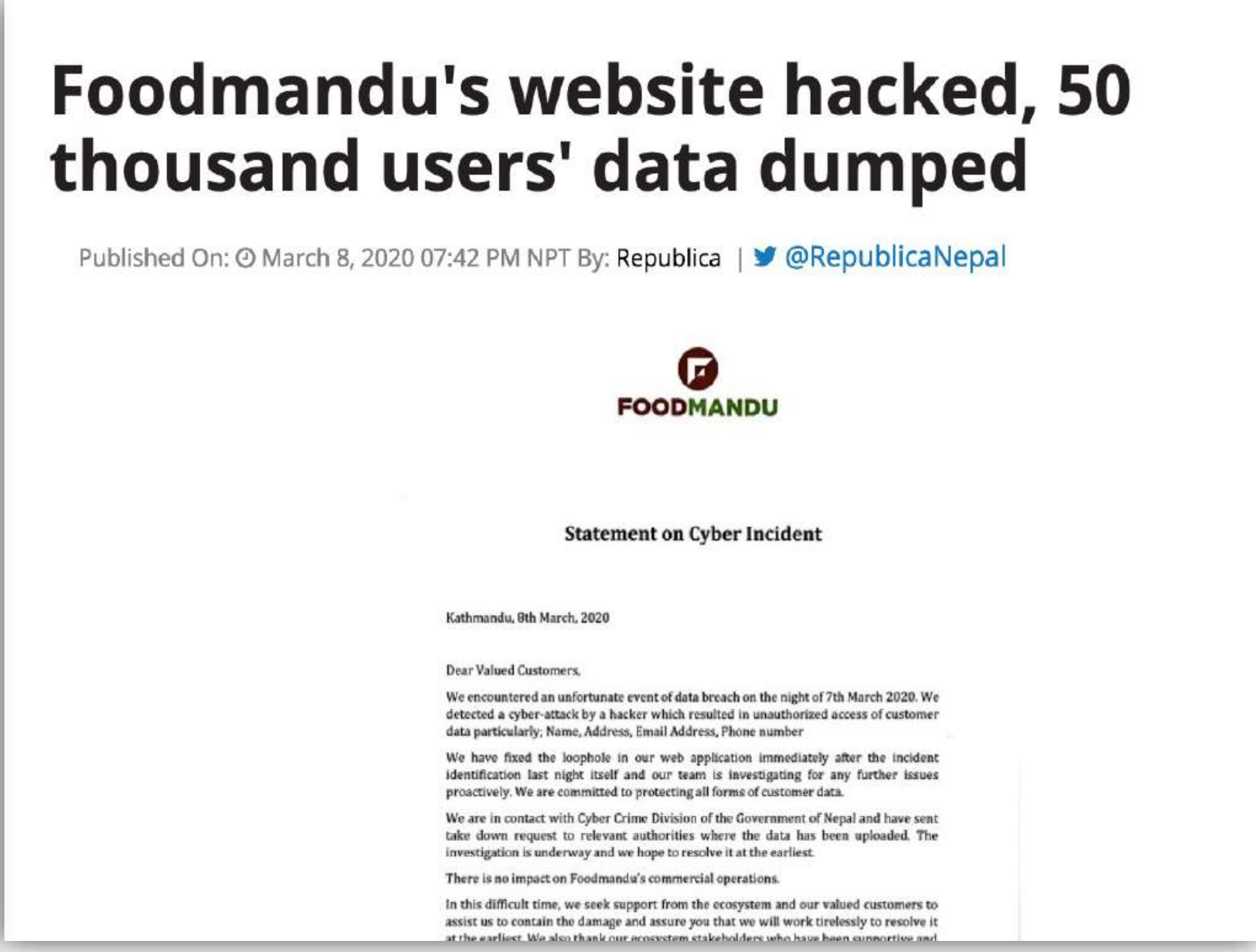
State of cyber security space



THE KATHMANDU POST

Vianet suffers data breach, leaking personal customer details online

Officials at Vianet confirmed the breach and said details of around 170,000 customers might have been leaked.



Foodmandu's website hacked, 50 thousand users' data dumped

Published On: March 8, 2020 07:42 PM NPT By: Republica | @RepublicaNepal

FOODMANDU

Statement on Cyber Incident

Kathmandu, 8th March, 2020

Dear Valued Customers,

We encountered an unfortunate event of data breach on the night of 7th March 2020. We detected a cyber-attack by a hacker which resulted in unauthorized access of customer data particularly; Name, Address, Email Address, Phone number

We have fixed the loophole in our web application immediately after the incident identification last night itself and our team is investigating for any further issues proactively. We are committed to protecting all forms of customer data.

We are in contact with Cyber Crime Division of the Government of Nepal and have sent take down request to relevant authorities where the data has been uploaded. The investigation is underway and we hope to resolve it at the earliest.

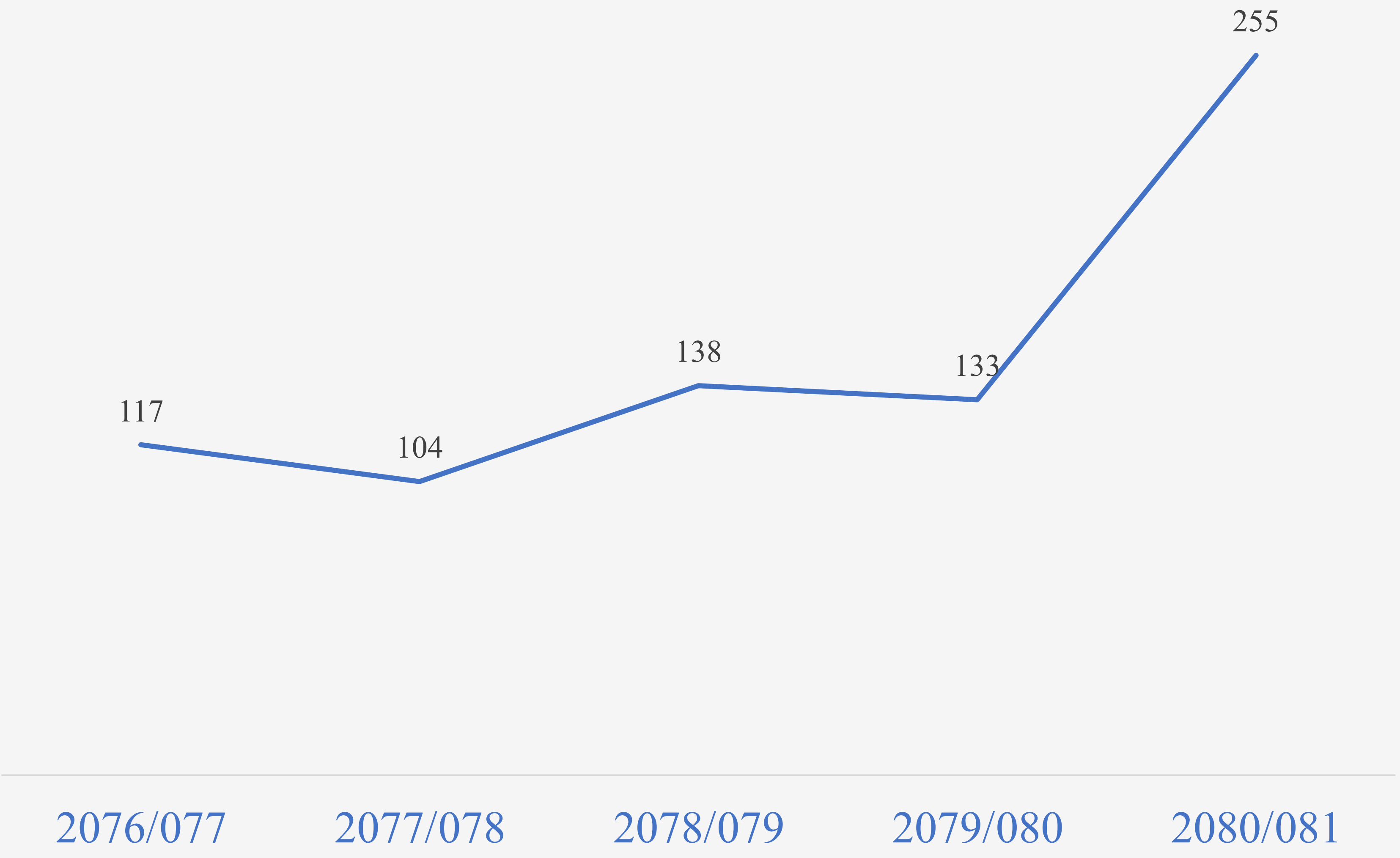
There is no impact on Foodmandu's commercial operations.

In this difficult time, we seek support from the ecosystem and our valued customers to assist us to contain the damage and assure you that we will work tirelessly to resolve it at the earliest. We also thank our ecosystem stakeholders who have been supportive and

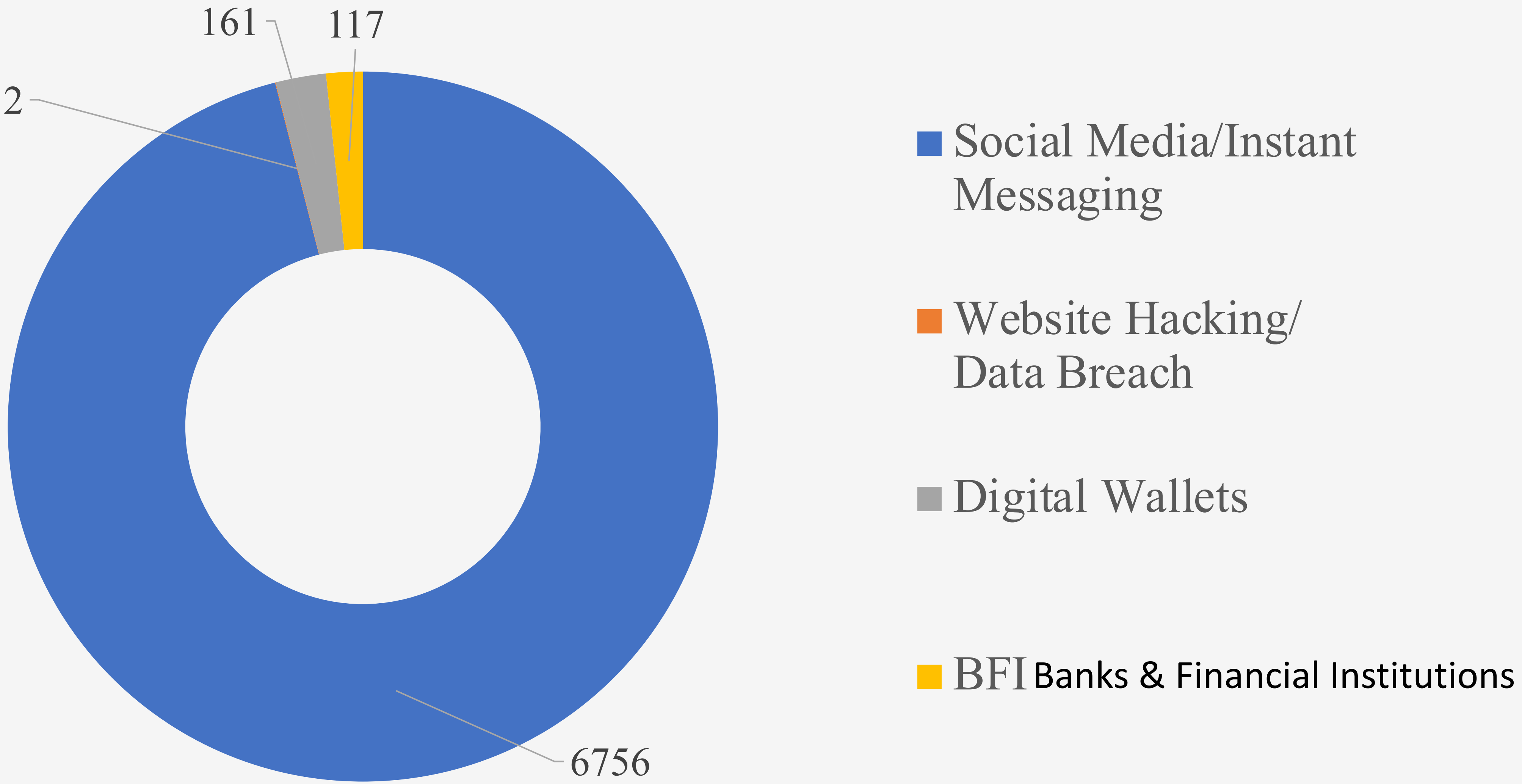
Role of Nepal Police in

Cyber security

Registered Cyber Crime cases in Last 5 Years



Patterns of Registered Cyber Crimes (Recent)



Secured Public Services provided

by

Nepal Police

Secured public services provided by Nepal police

- **Mobile App**: Android/Apple supported, emergency number, Location track, Incident reporting, panic mode.
- **TVRS (Traffic Violation Record System** : online E-chalaan, No need to carry Lic.
- **OPCR (Online Police Clearance Report)** : provides online Police Report within 3 days.

Security Challenges In Digital Era

Security Challenges

- Budgetary Issues
- Lack of Skilled Manpower
- Lack of Training
- Lack of state-of-the-art security devices
- Lack of Global Certifications

Network Security Recommendations

Enhancing Security: Recommendations

- Robust Network Architecture
- Fulfillment of Human Resources
- Latest CVEs Patches for software & system
- License/Genuine Software
- Regular IS Audit and Assessment
- Backup and Disaster Recovery

Enhancing Security: Recommendations

- Security Awareness training
- Implement **security framework**
- ***Central Security Gateway*** and **Content level Filtering.**

Cyber Security Awareness Video

To know about Cyber Security

Thank You !