# Cyber Hygiene Awareness: Protecting Your Digital Life

সাইবার হাইজিন সচেতনতা বিষয়ক এই গুরুত্বপূর্ণ আলোচনা সভায়   সকলকে স্বাগতম। আমরা দেখব কেন আমাদের ডিজিটাল জীবন রক্ষা করা অত্যন্ত গুরুত্বপূর্ণ, বিশেষ করে শিক্ষার্থীদের জন্য। তোমাদের ডিভাইসগুলি সুরক্ষিত করতে, সংবেদনশীল ডেটা সুরক্ষিত করতে জানতে হবে।

**Sourav Mazumder**
**Librarian, Ghoksadanga Birendra Mahavidyalaya**

# What is Cyber Hygiene?

### সংজ্ঞা

সাইবার হাইজিন মানে আমাদের ডিজিটাল ডিভাইসের নিরাপত্তা বজায় রাখা। এটা আমাদের প্রযুক্তির জন্য ব্যক্তিগত পরিষ্কার-পরিচ্ছন্নতার মতো।

### সাদৃশ্য

যেমন হাত ধোয়া অসুখ থেকে বাঁচায়, তেমনি ভালো সাইবার অভ্যাস অনলাইনের ঝুঁকি কমায়। এটা আমাদের ডিজিটাল দুনিয়াকে নিরাপদ রাখে।

### উদ্দেশ্য

আমাদের লক্ষ্য হলো সাইবার হুমকির ঝুঁকি কমানো। এর মধ্যে শক্তিশালী পাসওয়ার্ড ব্যবহার এবং সফটওয়্যার আপডেট রাখা অন্তর্ভুক্ত।

# Why Cyber Hygiene Matters

## দিন দিন বেড়ে চলেছে ইন্টারনেটভিত্তিক অপরাধ

ভারতের দ্রুত ডিজিটাল রূপান্তর একদিকে অগ্রগতির সম্ভাবনা তৈরি করলেও, অন্যদিকে সাইবার অপরাধের ঝুঁকি বাড়িয়ে তুলছে, যার ফলে আইটি, স্বাস্থ্য, উৎপাদন, আর্থিক খাত ও ক্ষুদ্র ব্যবসাগুলি লক্ষ্যে পরিণত হচ্ছে। সরকারি উদ্যোগ (যেমন I4C ও NCRP) থাকলেও, সাইবার সচেতনতার অভাব, দুর্বল পরিকাঠামো ও সাইবার নিরাপত্তায় বিনিয়োগের ঘাটতির কারণে চ্যালেঞ্জ রয়ে যাচ্ছে।

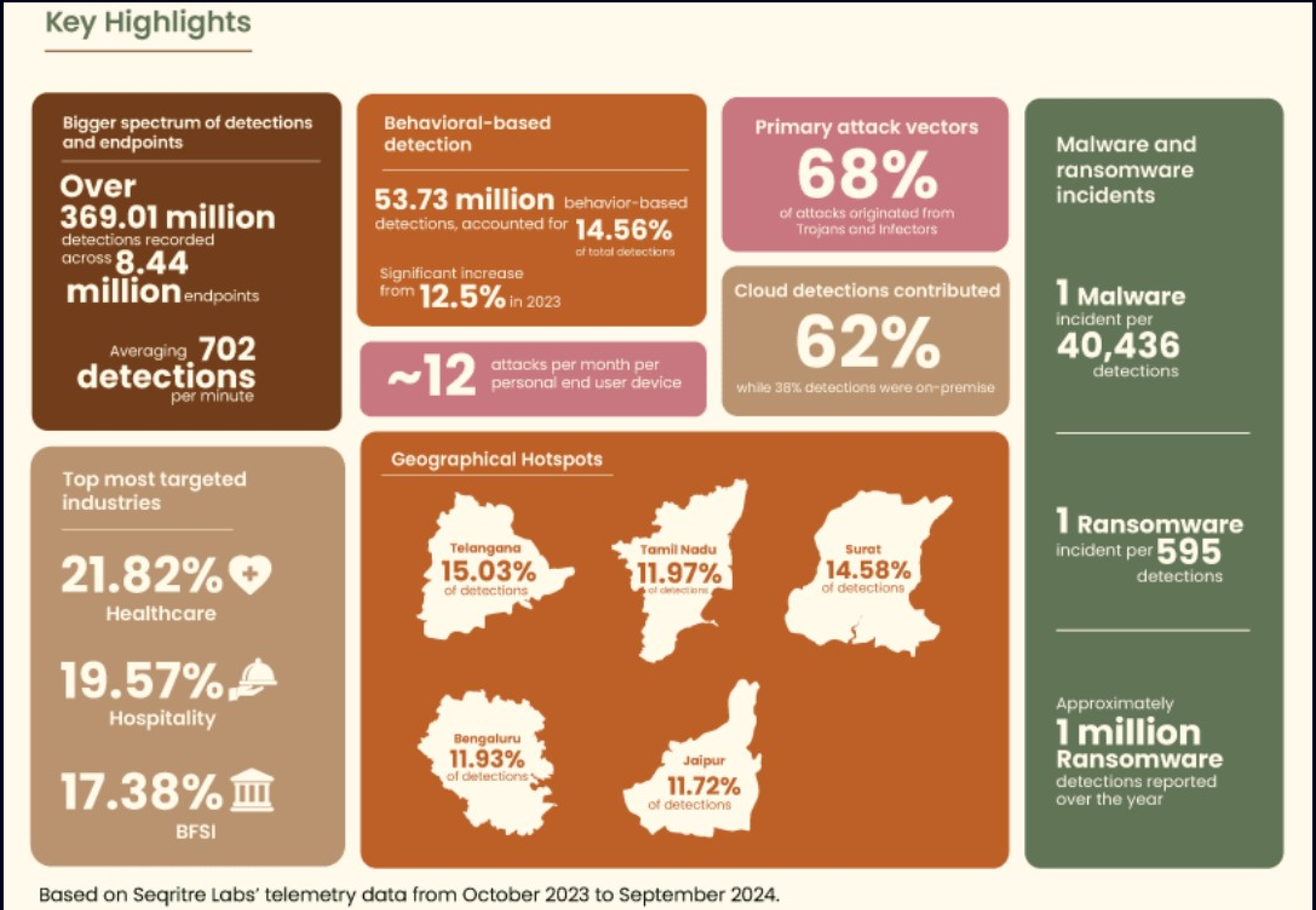
## সোশ্যাল মিডিয়ার ঝুঁকি

সোশ্যাল মিডিয়ায় ভুয়া প্রোফাইল ও ফিশিং প্রতারণা খুবই সাধারণ – সচেতন থাকুন, নিরাপদ থাকুন।

## শিক্ষা ও পেশাগত জীবনের প্রভাব

পড়াশোনার কাজ ও অনলাইন পরিচিতি রক্ষা করা জরুরি। ডেটা সুরক্ষা ভবিষ্যতের ক্যারিয়ারে প্রভাব ফেলতে পারে।

# India Cyber Threat Report 2025



# Passwords: The First Line of Defense

### Strong & Unique

প্রতিটি অ্যাকাউন্টের জন্য আলাদা ও শক্তিশালী পাসওয়ার্ড ব্যবহার করা উচিত, যা অন্তত ১২ অক্ষরের হবে এবং তাতে বড় হাতের ও ছোট হাতের অক্ষর, সংখ্যা এবং প্রতীক থাকবে।

### Password Managers

LastPass বা 1Password-এর মতো টুল ব্যবহার করা যেতে পারে, যেগুলি নিরাপদভাবে জটিল পাসওয়ার্ড সংরক্ষণ ও তৈরি করতে সাহায্য করে।

### Two-Factor Authentication

সম্ভব হলে সর্বদা 2FA (Two-Factor Authentication) চালু করা উচিত, কারণ এটি শুধুমাত্র পাসওয়ার্ডের বাইরে অতিরিক্ত একটি সুরক্ষা স্তর যোগ করে।

# Software Updates: Keep Your Devices Healthy

### Security Patches

আপডেট ডিভাইসের সুরক্ষার জন্য জরুরি, কারণ এগুলি নিরাপত্তাজনিত ত্রুটি মেরামত করে।

### Bug Fixes

আপডেট সফটওয়্যারের সমস্যা ঠিক করে এবং ডিভাইস ভালোভাবে কাজ করে।

### Automatic Updates

ডিভাইস সুরক্ষিত রাখতে সব সিস্টেমে অটো আপডেট চালু করে রাখা দরকার।

### Avoid Outdated Software

# Safe Browsing Habits

## Avoid Suspicious Links

অজানা লিংকে ক্লিক করা উচিত নয়। ওয়েবসাইটে “HTTPS” ও তালা চিহ্ন আছে কিনা তা যাচাই করে নেওয়া উচিত

## Use Antivirus Software

অ্যান্টিভাইরাস সফটওয়্যার ইনস্টল করা উচিত। Norton, McAfee বা Bitdefender ভালো বিকল্প হতে পারে।

## Scam Awareness

ভুয়া অনলাইন অফারের ব্যাপারে সচেতন থাকতে হবে। কেনাকাটার আগে সব সময় যাচাই করে নেওয়া উচিত।

## Beware of Phishing

ফিশিং ইমেইলের ব্যাপারে সাবধান থাকুন এবং নিরাপদ নয় এমন সাইটে ব্যক্তিগত তথ্য দেবেন না।

# Your connection is not private

Attackers might be trying to steal your information from **example.com** (for example, passwords, messages or credit cards). Learn more

NET::ERR_CERTIFICATE_TRANSPARENCY_REQUIRED

- [x] Help improve security on the web for everyone by sending URLs of some pages that you visit, limited system information, and some page content to Google. Privacy policy

Advanced

Back to safety

# Social Media Security

## Adjust Privacy Settings

নিজের পোস্ট কারা দেখবে তা ঠিক করে দিন এবং ব্যক্তিগত তথ্য কম শেয়ার করুন।

## Be Cautious of Oversharing

পোস্ট করার আগে ভাবুন, কারণ বেশি ব্যক্তিগত তথ্য শেয়ার করা বিপজ্জনক হতে পারে।

## Verify Friend Requests

অজানা অনুরোধ নিশ্চিত করুন, কারণ প্রতারকরা ভুয়া প্রোফাইল ব্যবহার করতে পারে।

## Report Suspicious Activity

অস্বাভাবিক আচরণ দেখলে তা সঙ্গে সঙ্গে রিপোর্ট করুন। নিজেকে এবং অন্যদের রক্ষা করুন।

# Public Wi-Fi Safety

### Avoid Sensitive Transactions

পাবলিক ওয়াইফাইতে ব্যাংকিং বা শপিং করা নিরাপদ নয়।

### Use a VPN

একটি VPN আপনার ডেটা এনক্রিপ্ট করে এবং নিরাপদ সংযোগ প্রদান করে।

### Verify Wi-Fi Network

নেটওয়ার্ক সঠিক কিনা দেখে নিন এবং নিরাপদ না এমন সংযোগ এড়িয়ে চলুন।

### Turn Off Auto-Connect

অটো ওয়াইফাই কানেকশন বন্ধ রাখুন যাতে অজানা নেটওয়ার্কে সংযোগ না হয়।

# Data Backup and Recovery

1

**Regularly Back Up**

ডেটা হারানোর থেকে বাঁচতে গুরুত্বপূর্ণ ফাইলগুলো সময়ে সময়ে সংরক্ষণ করুন।

2

**Cloud Storage**

Google Drive, Dropbox বা বাহ্যিক ড্রাইভে আপনার ফাইল সংরক্ষণ করুন।

3

**Test Backups**

ব্যাকআপ কাজ করছে কিনা পরীক্ষা করুন এবং ডেটা ফিরে পাওয়া যাবে কি না নিশ্চিত করুন।

4

Recovery Plan

ডেটা চুরি বা হারানোর পরিস্থিতির জন্য প্রস্তুতি নিন এবং র‍্যানসমওয়্যারের বিরুদ্ধে সাবধান থাকুন।

# Resources and Next Steps

1

Campus IT Support

2

Awareness Training

3

Online Courses

4

Stay Informed

# Thank You