महाराष्ट्र सायबर, मुंबई

CYBER SAFE WOMEN

सायबर युग

- आजच्या युगात इंटरनेट प्रत्येक व्यक्तीच्या जीवनाचा अविभाज्य भाग बनला आहे. दैनंदिन जीवनातले बरेच व्यवहार आजकाल इंटरनेटच्या माध्यमातून पार पाडले जातात. (जसे की आर्थिक व्यवहार, बँकिंग, व्यावसायिक, शैक्षणिक, वैद्यकीय व जनसंपर्क इत्यादी.)
- इंटरनेटच्या माध्यमाने मानवी जीवन सुलभ झाले आहे हे जितके खरे तितकेच याच्या अपुऱ्या माहितीने ते धोकादायक झाले आहे.
- सायबर साक्षरता ही एक महत्वाची बाब आहे जी एखाद्या व्यक्तीच्या सुरक्षिततेसाठी आवश्यक असते.
- आपण उत्तम रितीने मोबाईलचा वापर करतो पण याचा अर्थ असा नाही कि आपण सायबर साक्षर आहोत.

आपल्या दैनंदिन जीवनात येणारा इंटरनेटशी संबंध

- ❑ इंटरनेट बँकिंग
- ❑ ऑनलाईन खरेदी
- ❑ ऑनलाईन गेम्स (Games)
- ❑ मनोरंजन
- ❑ शिक्षण
- ❑ ऑनलाईन संवाद
- ❑ सोशल माध्यम

सायबर गुन्हे

- सायबर गुन्हे हे असे गुन्हे आहेत ज्यात संगणक, इंटरनेट किंवा मोबाईल तंत्रज्ञानाचा वापर करून वैयक्तिक पातळी वर किंवा संस्थांविरुद्ध कृत्य केले जाते.
- सायबर युगात सायबर गुन्हे करण्यासाठी सोशल नेटवर्किंग साइट्स, ई-मेल, चॅटरूम, पायरेटेड सॉफ्टवेअर, वेबसाइट इत्यादी सारख्या प्लॅटफॉर्मचा वापर केला जातो.
- मुले व महिला विविध प्रकारच्या सायबर क्राईमला बळी पडतात.

तुम्ही इंटरनेटवर सुरक्षित आहात का ?

सायबर सुरक्षिततेची गरज

- वैयक्तिक माहितीची सुरक्षा .
- आर्थिक नुकसान टाळण्यासाठी.
- विविध प्रकारच्या ऑनलाईन सुरक्षा :
  - बँकिंग (UPI, ATM PIN, OTP, CVV No.)
  - समाज माध्यम (WhatsApp, Instagram, Facebook etc.)
  - शैक्षणिक माध्यम (Byju's, Youtube, Unacademy, Diksha etc.)
  - पेमेंट Gateways (Google Pay, PayPal, Paytm, etc.)

सायबर गुन्ह्यांचे प्रकार

- सोशल इंजिनीयरिंग
- फिशिंग
- नोकरीचे लोभ दाखवून होणारी फसवणूक.
- लग्नाचे आमिष दाखवून होणारी फसवणूक.
- बँकिंग विषयी होणारी फसवणूक इत्यादी.

सोशल इंजिनीयरिंग

- लोकांना गोपनीय माहिती उघड करण्यासाठी पटवून देण्याची कला.
- आपली गोपनीय माहिती आपल्याकडून:
  - फोन
  - ई-मेल
  - व्यक्तीशः

  इत्यादी द्वारे घेतली जाते.

फिशिंग

- फिशिंगमध्ये आपले सोशल मीडिया, बँकिंग व ATM कार्डचे डिटेल्स मिळवण्याचा प्रयत्न केला जातो.
- मूळ संकेतस्थळासारखे दिसणारे बनावट संकेतस्थळ बनवून ग्राहकांना फसवून त्यांची संवेदनशील माहिती चोरण्यात येते.
- ई-मेल किंवा फोन मेसेज वरून बनावट वेबलिंक पाठवून आपली माहिती चोरण्यात येते .

टिप : https ने सुरुवात होणाऱ्या सुरक्षित website चा वापर करावा

नोकरीचे प्रलोभन दाखवून होणारी फसवणूक

JOB SCAM

Dear Candidate, Immediate Join!

Ref: "TATA INDIA LIMITED" - DIRECT RECRUITMENT'S OFFER.

It is our good pleasure to inform you, that you are selected for one of our given requirements. The Company has urgent openings for new Plants in **Delhi, Maharashtra, Gujarat, UP and Karnataka**. The Company required urgent staff for **Administration, IT/Computer and Production Department** as **Executives and Managers**. Fresher's / 0-5 year of experience willing to join within 15 days or after Completion of final face to face meeting with us.

The Company Tata Motors Ltd is the best it Company in India, the Company is recruiting the candidates for our new Plants in various cities. Your interview will be held at the Company Corporate office in Delhi on **10th of June 2014**, at **11.30** AM, you will be pleased to know that the **432** candidates shortlist selected by **465** candidates will be giving appointment, meaning that your Application can progress to final stage. You will have to come to the Company corporate office in Delhi, your offer letter with tickets will be sent to you by courier before date of interview. You have to come for interview with all required documents by Company HRD.

REQUIRED DOCUMENTS BY THE COMPANY HRD Fake list!

1) Photo-copies of qualification documents.
2) Photo-copies of experience certificates (if any)
3) Photo-copies of address proof Payment without proof!
4) Two Passport size photographs.

You have to deposit the (security) as an initial amount in favor of our company HR name in charges to collect your payment department for **Rs. 7,200/-** (Seven Thousand And Two Hundred Rupees Only) any **MERCANTILE BANK**, Branch from your Home City to our Company HR Name In-Charges. **(Managing Directors) A/c No. - 705710110000323, Mr. KAMAL SINGH**, this is refundable interview security. Your offer letter with Air tickets or Train tickets will be send to your Home Address by courier after receiving the confirmation of interview security deposited in any **MERCANTILE BANK**, and The Company will pay all the expenditure to you at the time of face-to-face meeting with you in Company. Fake promise!

The Job profile, salary offer, and date-time of interview will be mentioned in your offer letter. Your

अर्जंट जॉईन करण्या बाबत

खोटी यादी

Payment ची मागणी, पुरावा न घेता

खोटी आश्वासने

नोकरीचे/लॉटरीचे प्रलोभन दाखवून होणारी फसवणूक

- आपल्याला अज्ञात संकेतस्थळांकडून नोकरीची ऑफर मिळाल्यास प्रथम त्याची सत्यता पडताळून पहा.
- आपल्याला लॉटरीच्या ऑफर प्राप्त झाल्यास सावधगिरी बाळगा.
- लॉटरीची रक्कम मिळविण्यासाठी ऍडव्हान्स पैसे भरू नका.
- अज्ञात ईमेलमधील संलग्न फाईल किंवा लिंक उघडताना खबरदारी घ्या.

लग्नाचे आमिष दाखवून होणारी फसवणूक टाळण्यासाठी घ्यावयाची खबरदारी

- विवाहविषयक संकेतस्थळावर फसवणुकीच्या उद्देशाने गुन्हेगार खोट्या आकर्षक प्रोफाईल बनवतात.
- लग्न करण्याचे आमिष दाखवून त्या व्यक्तीशी जवळीक साधली जाते.
- पिडीत व्यक्तीला पैशांची मागणी किंवा एखादे गैरकृत्य करण्यास भाग पाडतात.

लग्नाचे आमिष दाखवून होणारी फसवणूक टाळण्यासाठी घ्यावयाची खबरदारी

- सोशल मीडियावरून मैत्री करताना सावधानता बाळगा.
- आपली संवेदनशील वैयक्तिक माहिती अज्ञात व्यक्तीला सांगू नका.
- सोशल मीडियावरील समोरच्या व्यक्तीचे प्रोफाइल तपासून बघावे.
- समोरच्या व्यक्तीचे प्रोफाइल तपासल्यावरच मैत्री करावी व खात्री केल्याशिवाय अशा माणसांना उधारीने पैसे देऊ नका.
- अज्ञात व्यक्तींबरोबर वैयक्तिक फोटो Share करू नका.

बँक विषयक फसवणूक टाळण्यासाठी घ्यावयाची खबरदारी

- आपल्या डेबिट / क्रेडिट कार्ड ची माहिती, १६ अंकी नंबर, पिन , ओटीपी क्रमांक इ. कोणालाही देऊ नका.
- लक्षात ठेवा! अशा माहितीसाठी बँक कधीही कॉल करत नाही.
- आपला पिन क्रमांक ए.टी.एम. किंवा इतर ठिकाणी प्रविष्ट करताना सावधानता बाळगा.
- एटीएमच्या वापरानंतर आपल्या एटीएम पावत्या नष्ट करा
- जर तुम्हाला काही संशयित मेसेज आले तर त्वरित तुमच्या बँकेत संपर्क साधा.

IDENTITY THEFT

- सार्वजनिक प्लॅटफॉर्मवर वैयक्तिक माहिती (जन्मतारीख, जन्मस्थान, पूर्वीचे नाव, कौटुंबिक तपशील, पत्ता, फोन नंबर) देऊ नका
- इंटरनेटचा वापर करताना आपल्या ओळख पत्रांची माहिती (आधार, पॅन, ड्रायव्हिंग लायसन्स) अनोळखी माणसांना किंवा सार्वजनिक प्लॅटफॉर्मवर देऊ नका.
- आपली वैयक्तिक माहिती मिळवून तो इतरांना आपण आहोत असे भासवून त्यांच्याशी चुकीच्या पद्धतीने संवाद साधू शकतो
- गुन्हेगार हा ई-मेल, मेसेज किंवा फोनद्वारे व्यक्तीची वैयक्तिक ओळख चोरी करतो.
- तुमचे ओळखपत्र सबमिट करताना त्यावर नेहमी कारण ,तारीख व स्वाक्षरी करावी.
- लकी ड्रॉ कुपन किंवा कोणताही फॉर्म भरताना काळजी घ्या!

Free Wi-Fi usage theme

- संवेदनशील खाजगी माहितीचा वापर करताना सार्वजनिक वाय-फाय चा वापर टाळा.
- सार्वजनिक वाय फाय वापरताना व्हर्च्युअल प्रायव्हेट नेटवर्क(VPN) वापरा.
- सुरक्षित ब्राउझिंगसाठी HTTPS वेबसाइट वापरा.
- स्मार्टफोनवरील स्वयंचलित (Automatic) वाय-फाय लॉग-इन बंद करा
- वाय-फाय साठी साइन अप करण्यासाठी संवेदनशील खाजगी माहिती देताना सावधगिरी बाळगा.

Passwords / Anti-virus

- नेहमीच एक सशक्त पासवर्ड वापरा जेणेकरून तो कोणाच्याही लक्षात येणार नाही.
- पासवर्ड नियमितपणे बदलत राहावे.
- आपला पासवर्ड कोणालाही सांगू नका.
- प्रत्येक अकाउंटसाठी वेगळा पासवर्ड वापरा.
- आपल्या कॉम्प्यूटरसाठी अँटीव्हायरस आणि फायरवॉलचा वापर करा.

महिला व बालकांसंदर्भात होणाऱ्या गुन्ह्यांचे प्रकार

चाईल्ड पोर्नोग्राफी

- १८ वर्षाखालील बालकांवर होणारा लैंगिक अत्याचार व त्याचे चित्रीकरण याला चाईल्ड पोर्नोग्राफी असे म्हणतात.
- लहान बालकांवर खाऊ, खेळणी इत्यादीचे आमिष दाखवून लैंगिक अत्याचार केले जातात.

सायबर ग्रुमिंग

- सोशल मिडिया किंवा मेसेजिंग प्लॅटफॉर्मद्वारे मुलांचे लैंगिक शोषण किंवा कोणत्याही प्रकारे शोषण करण्याच्या उद्देशाने जवळीक निर्माण केली जाते.
- सायबर ग्रुमर आपल्याला भेटवस्तू, प्रशंसा, मॉडेलिंग जॉबची ऑफर देतात आणि नंतर ते अश्लिल संदेश, छायाचित्रे किंवा व्हिडिओ पाठवू लागतात आणि आपल्या बरोबर लैंगिक सुस्पष्ट प्रतिमा किंवा व्हिडिओ पाठविण्यास सांगतात.

सायबर बुलींग

- सायबर बुलींग मध्ये स्त्रियांना व मुलांना धमकी देऊन त्यांना मानसिक त्रास दिला जातो.
- अश्लिल किंवा हानिकारक संदेश, टिप्पण्या आणि प्रतिमा / व्हिडिओ पाठवून एखाद्याला त्रास देण्यासाठी इंटरनेट किंवा मोबाईल तंत्रज्ञानाचा वापर केला जातो.
- सायबर गुन्हे करणारी व्यक्ती मजकुर संदेश, ई-मेल, सोशल मिडिया प्लॅटफॉर्म, वेबपृष्ठे, चॅटरूम्स इत्यादीचा वापर करतात.
- यामुळे विद्यार्थ्यांच्या शारीरिक, भावनिक, सामाजिक आणि मानसिक जीवनात गंभीर परीणाम होतात.

मॉर्फिंग

- मॉर्फिंग मध्ये एखाद्या व्यक्तीचे मूळ चित्र बदलले जाते.
- महिलांचे मूळ चित्र वेबसाईट वरून डाउनलोड करून, मॉर्फिंग करून, पुन्हा ते वेबसाईट वर रिपोस्ट/अपलोड करून फेक प्रोफाईल बनवली जाते.

सायबर डिफेमेशन [बदनामी]

- सायबर डिफेमेशन मध्ये एखाद्या व्यक्ती बाबत चुकीचे विधान करून त्याच्या सामाजिक प्रतिष्ठेला हानी पोहचवली जाते.
- उदाः एखाद्या व्यक्तीच्या सामाजिक प्रतिष्ठेला हानी पोहचविण्याच्या उद्धेशाने केलेले ई-मेल किंवा केलेली पोस्ट.

सायबर स्टॉकिंग

- एखाद्या व्यक्तीच्या online हालचालींचा पाठलाग करणे, त्यांच्यावर सतत लक्ष ठेवणे व त्याची वैयक्तिक माहिती गोळा करून ती सोशल मीडिया वर पोस्ट करणे.
- अशी संवेदशील माहिती गोळा करून सायबर स्टॉकर खालील प्रकारे दुरुपयोग करू शकतात जसे की नाव, कौटुंबिक पार्श्वभूमी, Mobile नंबर आणि पिडीतेच्या दैनंदिन व्यवहारामध्ये प्रवेश करुन, स्टॉकर पिडीतेच्या नावाने डेटिंग सेवांशी संबंधित वेबसाइटवर पोस्ट करतो.

ऑनलाईन गेमिंग

- मुले मोबाईल, संगणक, पोर्टेबल गेमिंग डिव्हाइसचा वापर करून सोशल नेटवर्क वर ऑनलाईन गेम खेळतात .

  उदा. BlueWhale, Momo challenge, Pub G.

- ऑनलाईन गेमिंगचा आतिरेक केल्यामुळे मुले चोरी, आत्महत्या यासारख्या गुन्ह्यांना बळी पडतात.

इट्स नॉट युवर फॉल्ट !!!

- घर आणि कामाच्या ठिकाणी केले जाणारे शोषण.
- इंटरनेट आणि मोबाइल फोनच्या वापराबाबत साक्षरतेचा अभाव.
- गैरवर्तन सहन करणे.
- समाजामध्ये बदनामीची भीती.

मुले व महिलांची सुरक्षा (१/२)

- लहान मुलांची पोर्नोग्राफी (Pornography) हा गंभीर स्वरूपाचा गुन्हा आहे व कठोर कारवाईस पात्र आहे.
- लहान मुलांच्या अश्लील चित्रफिती बनवणे, बाळगणे आणि त्याचे वितरण करणे हे कायद्याने गुन्हा आहे.
- जर तुम्ही मुलाचे किंवा स्त्रियांचे अत्याचार (Child /Woman Abuse) किंवा गैरवर्तनाने (Harassment)पिडीत असाल तर जवळच्या पोलीस ठाण्यात त्वरित तक्रार दाखल करा.
- आक्षेपार्ह मेसेज रिसिव्ह झाल्यास डिलिट करू नका, त्याचा वापर पोलिसांना पुरावा (Evidence) म्हणून होऊ शकतो.
- मुलांना सायबर सुरक्षेबाबत योग्य ते शिक्षण /माहिती द्या.

मुले व महिलांची सुरक्षा (२/२)

- पॅरेंटल कंट्रोल सॉफ्टवेअर वापरा.
- रात्री उशिरा मोबाईल किंवा लॅपटॉप वापरण्यावर मर्यादा ठेवा.
- मुले इंटरनेटवर कोणाच्या संपर्कात आहेत याचा मागोवा ठेवा.
- आपल्या मुलाची इंटरनेट Activity तपासा.
- आपली मुले ऑनलाईन Surfing करत असताना त्यामध्ये सहभागी व्हा.
- मुलांशी त्याच्या दैनंदिन Activity बाबत संभाषण करा.
- शाळा आणि महाविद्यालयांमध्ये विद्यार्थी व पालकांसाठी कार्यशाळा आयोजित केली पाहिजे.

सायबर गुन्हेगारीवर प्रतिबंधक उपाय (१/२)

- आपल्या कॉम्प्युटर कडे कधीही दुर्लक्ष करू नये. तुम्ही जागेवर नसताना कॉम्प्युटरची स्क्रीन लॉक्ड् असली पाहिजे.
- सॉफ्टवेअर Update ठेवले पाहिजे.
- महत्वाच्या फाईल्स साठी पासवर्डचा वापर करावा.
- Password कधीही Share करू नका.
- कॉम्प्युटरला/ Device ला एक मजबूत Password ठेवा आणि त्याला 2-Factor Authentication करा.
- महत्वाच्या फाईल्सचा बॅकअप घ्यावा.
- WhatsApp, Facebook, Instagram आदी समाज माध्यमांव्दारे स्वत:चे व कुटुंबियांचे सध्याचे लोकेशन Share करणे टाळा.

....

सायबर गुन्हेगारीवर प्रतिबंधक उपाय (२/२)

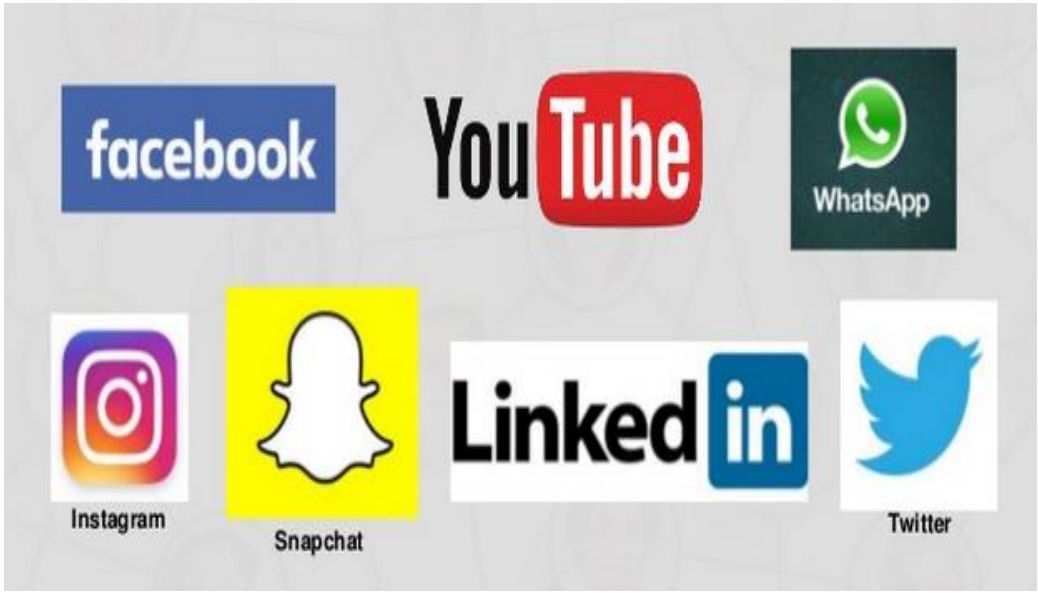
- पायरेटेड सिनेमा/गाणी डाउनलोड करू नका.
- वेबकॅम / मायक्रोफोन काम नसताना बंद ठेवा.
- वैयक्तिक डेटा Online share करू नका.
- आपल्या संगणकामध्ये Anti-Virus टाका.
- आपली Operating System वारंवार चेक करून त्याला Updated ठेवा.
- सिस्टिमचा फायरवॉल चालू ठेवा.
- Online भेटलेल्या अनोळखी व्यक्तीला प्रत्यक्षात भेटु नका/ संपर्क साधू नका.

मोबाईल फोन टिप्स

- नेहमीच एक सशक्त पासवर्ड वापरा.
- विश्वसनीय संकेत स्थळावरूनच ॲप डाउनलोड करावे.
- एकापेक्षा जास्त प्रमाणीकरण (मल्टिपल ऑथेंटिकेशन/ 2-Factor Authentication) असावे.
- बँक किंवा इतर महत्वाच्या ॲप्सला ॲप-लॉक वापरावे.
- आपले पासवर्ड मोबाईल मध्ये स्टोअर करू नये.
- विविध ॲप्सला देण्यात आलेल्या परवानग्या नियमितपणे तपासा.

सोशल मीडिया

- नवीन डिव्हाईस मधून लॉग-इन (Log-in) केले असल्यास वापर झाल्यावर नेहमी लॉग-आऊट (Log-out) करा.
- सोशल मीडियावरती तुमचे स्थान व इतर गोष्टी (Activity) शेयर करू नका.
- वाईट किंवा चुकीची पोस्ट अपलोड, शेअर आणि लाइक करू नका.
- आपल्या खात्याची गोपनीयता आणि सुरक्षिततेबाबत (Privacy and Security) काय दक्षता घ्यावी ह्याची माहिती ठेवा.



माहिती तंत्रज्ञान कायदा 2000

गुन्हा	कलम
संगणकातील कोड किंवा प्रोग्राम या मध्ये फेरफार करणे	कलम ६६
चोरलेली संगणक साधनसामुग्री अप्रामाणिकपणे वापरणे.	कलम ६६ब
ओळखदर्शक गोष्टींची (Identity Theft) चोरी केल्यास	कलम ६६ क
खाजगीपणाचे उल्लंघन केल्यास	कलम ६६ इ
सायबर दहशतवाद पसरविल्यास	कलम ६६ फ

माहिती तंत्रज्ञान कायदा 2000

गुन्हा	कलम
अश्लील मजकूर इलेक्ट्रॉनिक स्वरुपात प्रसिद्ध केल्यास किंवा पाठविल्यास	कलम ६७
लैंगिक भावना उत्तेजीत करणारे साहित्य इलेक्ट्रॉनिक स्वरुपात प्रसिद्ध केल्यास	कलम ६७ अ
कामवासना उत्तेजीत करणारी कृती इत्यादीमध्ये लहान मुलांचे चित्रण केलेले साहित्य इलेक्ट्रॉनिक स्वरुपात प्रसिद्ध केल्यास (Child Pornography)	कलम ६७ ब
मध्यस्थाद्वारे माहितीचे जतन केल्यास व धारण केल्यास (Man in the Middle Attack)	कलम ६७ क

लैंगिक अपराधांपासून बालकांचे संरक्षण अधिनियम, (POCSO) २०१२

- लैंगिक हमला, लैंगिक सतवणूक व संभोगचित्रण अशा अपराधांपासून बालकांचे संरक्षण करण्यासाठी लैंगिक अपराधांपासून बालकांचे संरक्षण अधिनियम, (POCSO) २०१२ हा कायदा अमलात आलेला आहे.
- वाढता बाल लैंगिक अत्याचार अपराध रोखण्यासाठी २०१९ ला कायदामध्ये सरकारने शिक्षेत वाढ केली आहे.

उदा:

Section 4 मध्ये तुरुंगवासाची शिक्षा ७ वर्षा ऐवजी १० वर्ष केली आहे.

रिपोर्टिंग पोर्टल

- आपल्याला बँकिंग किंवा संवेदनशील वैयक्तिक माहिती विचारणारे कोणतेही फसवे एसएमएस, ई-मेल, फोन कॉल प्राप्त झाल्यास, महाराष्ट्र सायबरच्या **www.reportphishing.in** या पोर्टलवर तात्काळ रिपोर्ट करा.
- सायबर गुन्हे नोंद करण्यासाठी, **https://cybercrime.gov.in** या संकेत स्थळावर तक्रार नोंदवा.
- आपला मोबाईल चोरी झाल्यास किंवा हरवल्यास मोबाईलचा IMEI क्रमांक ब्लॉक करण्यासाठी, **www.ceir.gov.in** या संकेतस्थळावर रिपोर्ट करा.
- आपल्या मोबाईलचा १५ अंकी IMEI क्रमांक ***#06#** डायल करून नोंद करून ठेवा
- महिला आणि बालकांसाठी सायबर गुन्ह्यांच्या तक्रारी करीता Toll Free Helpline Number **155260**

धन्यवाद!!