महाराष्ट्र पोलीस

सायबर गुन्हे व सुरक्षा

संकल्पना श्री. दत्तात्रय कराळे (भा.पो.से.)

विशेष पोलीस महानिरीक्षक, नाशिक परिक्षेत्र

वरील साधनांच्या सहाय्याने

१) आर्थिक फसवणूक करणे

२) ऑनलाईन धमकी देणे

३) एखाद्या व्यक्तीची बदनामी करणे

४) गोपनीय माहिती चोरणे

५) ऑनलाईन छळवणुक करणे

६) अश्लील मजकूर तयार करणे /प्रसारीत करणे

७) बाल लैंगिक शोषण

८) सायबर दहशतवाद

सायबर क्राईमचे प्रकार

Cyber Bullying

संगणक, मोबाइल फोन, लॅपटॉप इत्यादी इलेक्ट्रॉनिक किंवा संवाद साधण्याच्या साधनांचा वापर करून होणारी छळवणूक किंवा धमकावणे

Cyber Grooming

एखादी व्यक्ती एखाद्या अल्पवयीन मुला किंवा मुलीशी ऑनलाइन नातं निर्माण करून त्याला/तिला लैंगिक कृत्य करण्यासाठी फसवते किंवा दबाव आणते.

Child Pornography

बाल लैंगिक छळ करणारी सामग्री (CSAM) म्हणजे अशी कोणतीही सामग्री जी लैंगिक प्रतिमा स्वरूपात असते आणि ज्यामध्ये एखाद्या मुलाचे लैंगिक शोषण किंवा अत्याचार दाखवलेले असते.
माहिती तंत्रज्ञान कायद्याच्या कलम ६७ (B) नुसार, लैंगिक कृती करत असलेल्या मुलांचे वशळिलींळेप असलेली सामग्री इलेक्ट्रॉनिक स्वरूपात प्रकाशित करणे किंवा प्रसारित करणे हे दंडनीय आहे.

Cyber Stalking

सायबर स्टॉकिंग म्हणजे एखाद्या व्यक्तीने इलेक्ट्रॉनिक संवादाच्या माध्यमातून दुसऱ्या व्यक्तीचा पाठलाग करणे, ती व्यक्ती स्पष्टपणे नकार दर्शवत असता नाही तिच्याशी वैयक्तिक संपर्क साधण्याचा वारंवार प्रयत्न करणे.
एखाद्या व्यक्तीची प्रोफाईल वारंवार पाहणे, प्रोफाईल मधील फोटो, व्हिडीओ डॉऊनलोड करणे, त्यावर वारंवार कमेंट करणे.

Online Sextortion

ऑनलाइन सेक्स्टॉर्शन म्हणजे जेव्हा एखादी व्यक्ती इलेक्ट्रॉनिक माध्यमाचा वापर करून एखाद्याच्या खाजगी आणि संवेदनशील सामग्रीचा (व्हिडीओ, फोटो)प्रसार करण्याची धमकी देते, त्या बदल्यात आर्थिक मागणी, शारिरिक संभोग इत्यादीची मागणी करते.

Identy Theft

दुसऱ्या व्यक्तीच्या इलेक्ट्रॉनिक स्वाक्षरी, पासवर्ड किंवा इतर कोणत्याही अद्वितीय ओळख वैशिष्ट्यांचा अप्रामाणिकपणे वापर करून फसवणुक करणे.

Job Fraud

रोजगाराच्या शोधात असलेल्या लोकांना अधिक पगाराची आणि चांगल्या नोकरीची खोटी आश्वासने देऊन फसवण्याचा प्रयत्न.

Online Transaction Fraud

खोट्या वेबसाइट्स, बनावट पेमेंट लिंक, OTP/पासवर्ड चोरणे, किंवा फसव्या व्यवहाराच्या माध्यमातून पैसे चोरी करणे.

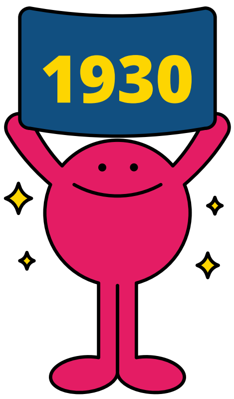
Debit/Credit Card Fraud

दुसऱ्या व्यक्तीच्या क्रेडिट किंवा डेबिट कार्डची माहिती त्याच्या परवानगीशिवाय वापरून खरेदी करणे किंवा त्यातून पैसे काढणे.

सायबर सुरक्षा

सायबर गुन्ह्याचे पिडीत असाल तर...

- जवळच्या पोलीस स्टेशनशी संपर्क साधा
- सायबर पोलीस स्टेशनशी संपर्क साधा
- REPORT ON THE NATIONAL CYBER CRIME PORTAL AT HTTPS://WWW.CYBERCRIME.GOV.IN
- NATIONAL CYBER CRIME HELPLINE NUMBER



आपल्याला सुरुवातीला जाणवत ही नाही की कोणी आपल्याला ऑनलाईन छळत आहे, हे तुम्हाला माहीत आहे का? सायबर बुली (ऑनलाईन छळ करणारा) हा एखादा ओळखीचा व्यक्ती, मित्र, नातेवाईक किंवा सोशल मिडिया, चॅट रूम, गेमिंग पोर्टल इत्यादीवर भेटलेला अनोळखी व्यक्तीही असू शकतो.सायबर बुलींगचा प्रमाण उग्र व अवहेलना करणारे संदेश पाठवण्यापासून, अपमानास्पद वागणुक देणे, अफवा पसरवणे, थेट धमक्या देणे, पाठलाग करणे अशा अनेक स्वरूपांमध्ये असू शकतो.

चला पाहूया की तुम्ही सायबर बुलींगपासून स्वतःचे संरक्षण कसे करू शकता.

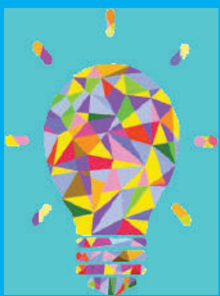
* सोशल मिडिया प्लॅटफॉर्मवर अनोळखी लोकांचे फ्रेंड रिक्वेस्ट स्वीकारू नका.
* तुमची वैयक्तिक माहिती जसे की जन्मतारीख, पत्ता, मोबाईल क्रमांक इत्यादी सोशल मिडिया किंवा इतर ऑनलाइन प्लॅटफॉर्मवर शेअर करू नका.
* सोशल मिडिया प्लॅटफॉर्मवरील प्रायव्हसी सेटिंग्जमध्ये जाऊन तुम्ही ठरवू शकता की कोण तुमचे पोस्ट्स पाहू शकतात.
* अनोळखी स्त्रोतांमधून डेटिंग ॲप्स, ऑनलाइन गेम्स वगैरे नको असलेले सॉफ्टवेअर आणि ॲप्स इंस्टॉल करू नका.
* चॅट रूममध्ये गप्पा मारताना खूप सावधगिरी बाळगा. कधीही तुमची वैयक्तिक माहिती शेअर करू नका.

तुम्ही स्वत: कधीही सायबर बुली होऊ नये, कारण हे कायद्याने शिक्षेस पात्र गुन्हा आहे.
त्यामुळे पीडित व्यक्तीवर मानसिक परिणाम होऊ शकतो.

जर तुम्ही सायबर बुलींगचे बळी असाल, तर काय करू शकता?

☞ तुमच्या पालकांना/मोठ्यांना तात्काळ कळवा.
☞ छळ करणाऱ्या व्यक्तीची ओळख पटवा.
☞ छळ करणाऱ्याला ब्लॉक करा.
☞ पोस्ट्स/संदेश जमा करा आणि सुरक्षित ठेवा.
☞ कधीही छळ करणाऱ्याला आक्रमकपणे उत्तर देऊ नका.
☞ जर तुमचे पालक किंवा वडीलधारी व्यक्तींना गरज वाटली, तर ते स्थानिक पोलिस ठाण्यात जाऊन छळ करणाऱ्याविरोधात तक्रार दाखल करू शकतात.

Cyber Grooming



सायबर ग्रूमिंग ही मुलं आणि किशोरवयीन मुलांना भेडसावणाऱ्या प्रमुख सायबर धोक्यांपैकी एक म्हणून समोर येत आहे.
यामध्ये एखादी व्यक्ती सामाजिक मीडिया किंवा मेसेजिंग प्लॅटफॉर्मच्या माध्यमातून मुलांशी भावनिक संबंध निर्माण करते, त्यांचा विश्वास संपादन करून त्यांचे लैंगिक शोषण किंवा फसवणुक करते.
सायबर ग्रूमर्स गेमिंग वेबसाइट्स, सोशल मीडिया, ईमेल, चॅट रूम्स, इन्स्टंट मेसेजिंग इत्यादींचा वापर करून खोटे खाते तयार करतात आणि स्वतःला मुलासारखे किंवा त्या मुलाच्या आवडी-निवडीसारखे असल्याचे भासवतात.

सुरुवातीला सायबर ग्रूमर तुमचं कौतुक करेल, भेटवस्तू देईल, मॉडेलिंगच्या कामाची ऑफर देऊ शकतो आणि नंतर अश्लील संदेश, फोटो किंवा व्हिडिओ पाठवायला सुरुवात करेल. नंतर तो तुम्हाला तुमचे लैंगिकदृष्ट्या स्पष्ट फोटो किंवा व्हिडिओ पाठवण्यासाठी सांगू शकतो.

चला पाहूया की तुम्ही सायबर बुलींगपासून स्वतःचे संरक्षण कसे करू शकता.

* सोशल मिडिया प्लॅटफॉर्मवर अनोळखी लोकांचे फ्रेंड रिक्वेस्ट स्वीकारू नका.
* तुमची वैयक्तिक माहिती जसे की जन्मतारीख, पत्ता, मोबाईल क्रमांक इत्यादी सोशल मिडिया किंवा इतर ऑनलाइन प्लॅटफॉर्मवर शेअर करू नका.
* ओळखीनंतर अल्प कालावधीतच जर एखादी व्यक्ती तुमच्या दिसण्याबद्दल खूप compliments देत असेल, तर सतर्क राहा.
* जे लोक तुमच्या शरीरिक किंवा लैंगिक अनुभवांबद्दल प्रश्न विचारतात, अशा लोकांशी बोलणं टाळा.
* जे लोक तुम्हाला अश्लील फोटो किंवा व्हिडिओ शेअर करण्यास सांगतात, अशा लोकांशी बोलू नका. जर तुम्ही असे फोटो किंवा व्हिडिओ कुणाशी शेअर केले, तर ती व्यक्ती ते इतरांशी शेअर करू शकते किंवा सोशल मीडियावर टाकू शकते. ते तुम्हाला ब्लॅकमेलही करू शकतात.
* ऑनलाइन भेटलेल्या कोणत्याही व्यक्तीला एकट्याने भेटायला जाऊ नका. नेहमी एक मित्र किंवा मोठ्या व्यक्तीला सोबत घेऊन जा.
* अनोळखी स्रोतांमधून डेटिंग ॲप, ऑनलाइन गेम्स यांसारखे अनावश्यक सॉफ्टवेअर किंवा ॲप्स इन्स्टॉल करू नका.
* चॅट रूममध्ये वैयक्तिक माहिती शेअर करू नका आणि तुमची ओळख मर्यादित ठेवा.

ONLINE GAMING

* गेमिंग कन्सोल्स हे संगणकासारखेच काम करतात, जिथे तुम्हाला खाते तयार करावे लागते, लॉगिन करावे लागते, हेडसेट लावावे लागते, वेबकॅम किंवा इतर डिव्हाइसेस वापरावी लागतात. तुम्ही कोट्यवधी लोकांशी एकत्र खेळता, त्यांच्याशी बोलता, तुमचे विचार शेअर करता, मित्र होता, ग्रुप्स, टीम्समध्ये सामील होता इत्यादी.
* ऑनलाइन गेम्स खेळणं मजेशीर असू शकतं, पण त्यासोबतच काही धोकेही येतात.

तुम्हाला माहिती आहे का की ऑनलाइन गेम्स डाउनलोड करताना तुम्ही नकळत स्पॅम, व्हायरस किंवा मॅलिशस सॉफ्टवेअर देखील डाउनलोड करू शकता, जे तुमच्या संगणकावर, मोबाइल फोनवर किंवा गेमिंग कन्सोलवर वाईट परिणाम करू शकते?म्हणूनच, गेम्स नेहमी विश्वासार्ह आणि नामवंत वेबसाइटवरूनच डाउनलोड करावेत. कधीही पायरेटेड गेम्स किंवा सॉफ्टवेअर डाउनलोड/इंस्टॉल करू नका.

चला पाहूया की तुम्ही स्वतःचं संरक्षण कसं करू शकता:

* ऑनलाइन गेम्स खेळताना तुमचं वैयक्तिक माहिती जसं की नाव, जन्मतारीख, पत्ता आणि फोन नंबर इतर खेळाडूंशी शेअर करू नका.
* ऑनलाइन गेम खेळताना तुमचे किंवा तुमच्या पालकांचे क्रेडिट कार्ड/डेबिट कार्डचे तपशील कुणाशीही शेअर करू नका.
* फ्री ऑनलाइन गेमिंग वेबसाइट्स विश्वसनीय नाहीत, अशा वेबसाइट्सवरून गेम्स डाउनलोड करू नका. ईमेल, मेसेज किंवा पॉपअपमधून आलेल्या लिंकवर क्लिक करून गेम डाउनलोड करू नका. त्यामुळे व्हायरस किंवा मालवेअर डाउनलोड होऊ शकते,
* तुमच्या संगणकावर, स्मार्टफोनवर किंवा इतर डिव्हाइसेसवर चांगले अँटीव्हायरस सॉफ्टवेअर इन्स्टॉल करा.
* तुमचे पासवर्ड कुणाशीही शेअर करू नका. तुमच्या ऑनलाइन गेमिंग अकाउंटसाठी आणि इतर ऑनलाइन खात्यांसाठी क्लिष्ट पासवर्ड वापरा. पासवर्ड नियमित अंतराने बदलणं ही एक चांगली सवय आहे.
* ऑनलाइन गेम्स खेळताना व्हॉईस चॅट किंवा वेबकॅम वापरू नका.
* ऑनलाइन गेमिंगमधून ओळख झालेल्या कुठल्याही व्यक्तीला प्रत्यक्ष भेटण्यासाठी जाऊ नका.

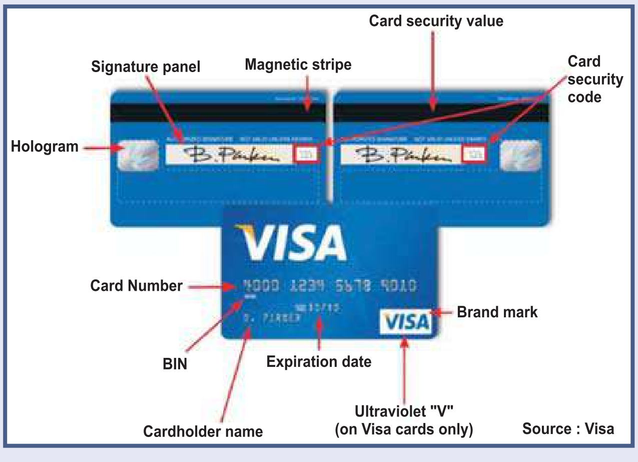
Online Transaction Fraud

डेबिट कार्ड, क्रेडिट कार्ड, नेट बँकिंग यासारख्या बँकिंग सेवांच्या माध्यमातुन फसवणुक...

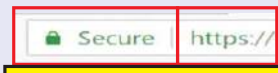
हे कसं कार्य करतं?

* सायबर गुन्हेगार ऑनलाइन फसवणूक करण्यासाठी अनेक पद्धती वापरतात.
* सायबर गुन्हेगार तुमच्या बँकेकडून किंवा क्रेडिट कार्ड सेवा पुरवठादाराकडून आलेल्या ईमेलसारखा एक बनावट ईमेल पाठवू शकतात. या ईमेलमधील लिंकवर क्लिक केल्यास तुम्हाला अशा पृष्ठावर नेलं जातं जिथे तुमची संवेदनशील माहिती जसं की बँक खाते तपशील, कार्ड तपशील, कार्ड व्हेरिफिकेशन व्हॅल्यू (CVV), एक्सपायरी डेट इत्यादी विचारली जाते.
* जर तुम्ही ही माहिती दिली, तर तुमचं खाते धोक्यात येऊ शकतं.

* कधीही तुमचे बँक आणि कार्ड तपशील जसे की ऑनलाइन अकाउंटचा पासवर्ड, कार्ड नंबर, CVV, एक्सपायरी डेट, PIN, OTP इत्यादी कुणाशीही शेअर करू नका.
* तुमच्या बँक खात्याचा ऑनलाइन पासवर्ड आणि डेबिट/क्रेडिट कार्डचा झखछ नियमितपणे अपडेट करण्याची सवय लावा.
* बँक खात्यात लॉगिन करताना नेहमी स्वत: बँकेची वेबसाईट टाइप करूनच लॉगिन करा.
* ईमेल, मेसेज किंवा पॉपअपमध्ये आलेल्या बँकेच्या लिंकवर क्लिक करू नका. ही लिंक बनावट असू शकते आणि ती तुम्हाला नकली वेबसाईटवर घेऊन जाऊ शकते. जर तुम्ही अशा बनावट साईटवरून लॉगिन केलं, तर तुमचे संवेदनशील तपशील जसे की खाते क्रमांक आणि पासवर्ड चोरी होऊ शकतात.



* तुम्ही सुरक्षित बँक वेबसाइटला भेट देत आहात याची खात्री करण्यासाठी बँकेच्या सिक्युरिटी सर्टिफिकेटच्या तपशीलांची आणि काही चिन्हांची तपासणी करा जसे की पत्त्याच्या ओळीत हिरव्या रंगाची रेषा, ॲड्रेस बारमध्ये लॉकचं चिन्ह आणि वेबसाईटचा पत्ता HTTPS ने सुरू होणं.



HOW TO SECURE DIGITAL PAYMENTS?

डिजिटल पेमेंटसाठी ओपन पब्लिक
Wi-Fi वापरू नका.

फोनमध्ये काय इन्स्टॉल करत
आहात याबाबत सतर्क राहा, विशेषत:
थर्ड पार्टी ॲप्सबाबत.

PIN नियमितपणे बदला.

डिव्हाइस हरवलं किंवा चोरी
झाल्यास तात्काळ रिपोर्ट करा.

अनधिकृत व्यवहार
झालाय का हे पाहण्यासाठी.
अकॉऊंट्स स्टेटमेंट नियमितपणे तपासा.

स्ट्राँग पासवर्ड निवडा म्हणजेच इंग्रजी
अक्षरं, संख्या आणि विशेष चिन्हांचा
(special characters) समावेश
असलेला पासवर्ड ठेवा, जेणेकरून तुमचं
अकॉऊंट आणि डेटा सुरक्षित राहील.

ई-वॉलेटचे लॉगिन तपशील व
वन टाइम पासवर्ड (OTP) कुणा
अनोळखी व्यक्तीशी शेअर करू नका.

ऑनलाइन खरेदी करताना दोन-स्तरीय
प्रमाणीकरण (Two-Factor Authentication)
सुरू आहे याची खात्री करा.

IDENTITY THEFT ?

VISHING

फसवणूक करणारी व्यक्ती तुम्हाला फोन करून स्वत:ला बँकेचा प्रतिनिधी म्हणून सांगू शकतात किंवा पैशांची मागणी करू शकतात.

PHISHING

स्कॅमर्स फसवणूक करणारे आणि हानीकारक ईमेल पाठवून तुमची गोपनीय माहिती चोरण्याचा प्रयत्न करू शकतात.

CLONING

गुन्हेगार तुमच्या क्रेडिट/डेबिट कार्डची माहिती कॉपी (क्लोन) करू शकतात.

स्वत:चं संरक्षण कसं कराल?

१. अनोखे, गुंतागुंतीचे पासवर्ड तयार करा, अक्षरे, संख्या आणि चिन्हे यांचा समावेश असलेले असावेत.
२. दोन-स्तरीय प्रमाणीकरण (Two-Factor Authentication) सुरू करा.

३. तुमचे आर्थिक खाते नियमितपणे तपासा.
४. तुमच्या बँक आणि क्रेडिट कार्ड खात्यांवर अलर्ट सेट करा.
५. अविश्वसनीय स्रोतांकडून आलेल्या लिंक्सवर क्लिक करू नका.

६. तुमची वैयक्तिक माहिती कुणालाही देऊ नका.
७. कागदपत्रे फाडून टाका, नष्ट करा.
८. बिल भरण्याची पद्धत म्हणून पेपरलेस (ई-बिलिंग) पर्याय निवडा.

REPORT ON THE NATIONAL CYBER CRIME PORTAL AT
HTTPS://WWW.CYBERCRIME.GOV.IN

IDENTITY THEFT

PROTECT YOUR PERSONAL DATA

- सोशल नेटवर्किंग साइट्सवर वैयक्तिक माहिती मर्यादित ठेवा.
- तुमच्या सर्व ऑनलाइन आणि सोशल नेटवर्किंग खात्यांची नियमितपणे तपासणी करा.
- प्रत्येक वेबसाइटवर उपलब्ध असलेल्या सुरक्षाविषयक सुविधांचा अवश्य वापर करा.
- जे दस्तऐवज तुम्ही पाठवत आहात, त्यांना पासवर्ड प्रोटेक्शन द्या.
- केवळ सुरक्षित पेमेंट गेटवे असलेल्या वेबसाइट्सवरूनच ऑनलाइन खरेदी करा.
- तुमच्या आर्थिक खात्यांमध्ये संशयास्पद व्यवहार होतोय का, यासाठी नियमितपणे तपासणी करा.
- क्रेडिट/डेबिट कार्ड वापरताना आणि PIN नंबर टाकताना आजूबाजूच्या लोकांपासून सावध राहा.
- फक्त विश्वासार्ह कंपन्यांशी किंवा वेबसाइट्सशीच व्यवहार करा.
- नेहमी गोपनीयता धोरण (Privacy Policy) वाचा आणि नीट समजून घ्या.
- तुमची वैयक्तिक माहिती चुकीच्या पद्धतीने वापरली गेली आहे असं वाटल्यास, तात्काळ उपाययोजना करा.

NATIONAL CYBER CRIME HELPLINE NUMBER

CHILD PORNOGRAPHY
and it's implications

ऑनलाइन अश्लील सामुग्रीशी संपर्क

1 अश्लील कार्टुन

2 इंस्टंट मेसेजिंग

3 चॅट रूम

4 चित्रपट

5 फोटो, व्हिडीओ शेअरींग प्लेटफॉर्म

6 ऑनलाईन गेम्स

7 सोशल मिडीया

8 ई-मेल

1
हे काय आहे?
त्यांना अश्लीलता (पोर्नोग्राफी) म्हणजे काय असते,
याची स्पष्ट आणि योग्य माहिती असणे आवश्यक आहे.

2
हे हानिकारक का आहे?
अश्लील सामग्री त्यांचं कोवळं मन आणि विचारविश्व बिघडवू शकते.
अश्लीलता त्यांच्या मानसिक, सामाजिक आणि भावनिक विकासावर वाईट परिणाम करू
शकते.हे त्यांच्या नातेसंबंधांवर, आत्मविश्वासावर आणि वागणुकीवरही परिणाम करू शकते.

3
त्याला नकार कसा द्यायचा?
Turn, Run and Tell!"
Turn away from the bad picture,
hurry and get away,
and go tell a trusted adult

डिजिटल अटक (Digital Arrest) घाबरू नका!

डिजिटल अटक (Digital Arrest) म्हणजे फसवणुकीचा एक प्रकार, ज्यात सायबर गुन्हेगार आपल्याला पोलीस, ईडी किंवा सीबीआय अधिकारी असल्याचं भासवून, फोन किंवा व्हिडिओ कॉल करतात. ते आपल्याला काही बेकायदेशीर कामात अडकल्याचं सांगून, अटक वॉरंट जारी झाल्याचं बतावून धमक्या देतात आणि पैशाची मागणी करतात.

Digital Arrest - 1

https://www.youtube.com/watch?v=RQ46CJBe3NQ

Digital Arrest - 2

https://www.youtube.com/watch?v=Hrb0qrpqQUo

Digital Arrest - 3

https://www.youtube.com/watch?v=QaniOYQDvsQ

सोशल मिडिया सुरक्षा

**Social media isn't your personal diary.
Avoid posting every life update online &
keep your personal details private.**

WhatsApp Security Checklist

Privacy Settings –

These settings limit who can access your personal information and activity on WhatsApp.

- **Last Seen** - Set to "Nobody" or "My Contacts" to prevent strangers from knowing when you were last active.
- **Profile Photo** - Choose "My Contacts" or "Nobody" to control who can view your photo.
- **Status Updates** - Customize visibility using "My Contacts" or "My Contacts Except..." to exclude specific people.
- **About** - Control who can see your "About" information, such as your bio. Set it to "Nobody", "My Contacts", or "My Contacts Except..."
- **Live Location** - If you're sharing your location, always double-check who has access and remove access when no longer needed.

Advanced Settings –

These settings add additional layers of protection for your WhatsApp communications.

- **Protect IP Address in Calls** - Enable this setting to prevent hackers from tracking or targeting your IP address during voice or video calls.
- **Disable Link Previews** - Enable this setting to prevent WhatsApp from automatically showing previews of links shared in messages, which can help you avoid malicious links.

Go to Settings > Go to "Privacy" >Scroll down to "Advanced" and click > Here click on both "Protect IP address in calls" and "Disable link previews"

Enable Two-Step Verification (2FA) –

Two-step verification adds an extra layer of security, requiring both your SIM card (or phone) and a PIN to log into WhatsApp.

Go to Settings > Account > Two-step Verification > Enable.

- **PIN** - Choose a 6-digit PIN that you'll need to enter when setting up WhatsApp on a new device.
  Go to Settings > Account > Passkeys.
- **Email Address** - Provide an email address for recovery purposes in case you forget your PIN.
  Go to Settings > Account > Email address.

Additional Security Measures –

Here are more ways to enhance your security and protect your account from threats.

- **Media Auto Download** - Disable Media Auto Download i.e. Photo, Audio, Video, Documents.

  Go to Settings > Storage and Data > Media auto-download > Disable.
- **Verify Unknown Contacts** - Always be cautious when receiving messages from unfamiliar contacts. If possible, verify the person's identity before sharing sensitive information.
- **Regular App Updates** - Ensure your WhatsApp app is always up to date. Developers frequently release updates that address security vulnerabilities.
- **Beware of Third-Party Apps** - Do not use unofficial WhatsApp versions or mods (e.g. WhatsApp Plus), as they can compromise your privacy and security.
- **Encrypt Backup** - Enable end-to-end encryption for your WhatsApp backups to protect your chat history in the cloud.

  Go to Settings > Chats > Chat Backup > End-to-end Encrypted Backup.
- **Screen Lock/Authentication** - Consider enabling your device's screen lock (PIN, fingerprint, Face ID) to protect access to WhatsApp.

Regularly Monitor Security Settings –

It's important to periodically review your WhatsApp security settings to ensure they're up to date:

- **Check Devices Connected** - Go to Settings > Linked Devices to review and disconnect any devices you don't recognize.
- **Backup and Export Chats** - Regularly back up important chats, but be cautious about sharing sensitive information in messages or using cloud services.

Facebook / Instagram Security Checklist

इन्स्टाग्राम मध्ये खालील सेटिंग्स केल्यानंतर फेसबुक अकाऊंट देखील सुरक्षित होईल.

इन्स्टाग्राम मध्ये स्वतःची प्रोफाईल ओपन करा व वरील ३ डॉट / रेषांवर क्लिक करा.
"सेटींग ॲन्ड ॲक्टिव्हिटी" हे पेज ओपन होईल.

- "अकाऊंट प्रायव्हसी" या ऑप्शन मध्ये "प्रायव्हेट अकाऊंट" हा ऑप्शन एनेबल करा.
- "वेबसाईट परमिशन" या ऑप्शन मध्ये,
  - "ब्राऊझर सेटिंग्स" या ऑप्शन मध्ये "ॲटो फिल कॉन्टॅक्ट फॉर्म" व "ॲटो फिल पेमेंट फॉर्म" हे ऑप्शन डिसेबल करा. व "सेफ वेबसाईट ब्राऊझिंग" हा ऑप्शन एनेबल करा.
  - "मेसेज लिंक्स" या ऑप्शन मध्ये "ओपन इन एक्स्टर्नल ब्राऊझर" हा ऑप्शन एनेबल करा.
- "अकाऊंट सेंटर" या ऑप्शन मधील, "पासवर्ड ॲन्ड सिक्युरिटी" या ऑप्शन मध्ये,
  - "चेंज पासवर्ड" या ऑप्शन मध्ये स्ट्राँग पासवर्ड सेट करा.
  - "टु फॅक्टर ऑथेंटिकेशन" या ऑप्शन मध्ये फेसबुक आणि इन्स्टाग्राम अकाऊंट चे टु फॅक्टर ऑथेंटिकेशन एनेबल करा.
  - "सेव्ह लॉगिन" या ऑप्शन मध्ये "सेव्ह लॉगिन" हा ऑप्शन एनेबल करा.
  - "व्हेअर यु लॉग इन" या ऑप्शन मध्ये स्वतःचे फेसबुक व इन्स्टाग्राम अकाऊंट आपल्या डिव्हाईस व्यतिरिक्त आणखी कोठे लॉग इन आहे का हे दिसते. जर आपल्या डिव्हाईस व्यतिरिक्त इतर डिव्हाईस वर अकाऊंट लॉग इन असेल तर, ते डिव्हाईस लॉग आऊट करावे.
  - "लॉगिन अलर्ट" या ऑप्शन मध्ये स्वतःचे फेसबुक व इन्स्टाग्राम अकाऊंट लॉगिन केल्याबाबतचा अलर्ट येण्याकरिता एनेबल करा.
  - "सिक्युरिटी चेकअप" या ऑप्शन मध्ये स्वतःचे फेसबुक व इन्स्टाग्राम अकाऊंट सुरक्षित करण्याकरिता तेथील ऑप्शन एनेबल करा.
- "अकाऊंट सेंटर" या ऑप्शन मधील, "पर्सनल डिटेल्स" या ऑप्शन मध्ये, सध्या चालू असलेला मोबाईल क्रमांक अपडेट असल्याची खात्री करा.
- "अकाऊंट सेंटर" या ऑप्शन मधील, "युअर इन्फॉरमेशन ॲन्ड परमिशन" या ऑप्शन मधील "युअर ॲक्टिविटी ऑफ मेटा टेक्नॉलॉजी" या ऑप्शन मध्ये "मॅनेज फ्युचर ॲक्टिविटी" या ऑप्शन मध्ये "डिस्कनेक्ट फ्युचर ॲक्टिविटी" हा ऑप्शन एनेबल करा. व त्यानंतर "क्लिअर प्रिव्युअस ॲक्टिविटी" या ऑप्शन मध्ये क्लिअर करा.
  - हे केल्याने मेटा वेगवेगळया सोर्सेस ला डेटा देणे बंद होईल.
- वरील सेटींग केल्यावर पासवर्ड चेंज करा.

HOW TO BE CYBER VIGILANT?

DUE TO THE PRESENCE OF A PLETHORA OF CYBERCRIMES IN CYBER SPACE IT IS IMPORTANT FOR US TO BE CYBER VIGILANT.

KEEP SOFTWARES AND OPERATING SYSTEMS UPDATED

USE ANTIVIRUS SOFTWARE FOR YOUR DEVICES

SET YOUR SOCIAL NETWORKING PROFILES TO PRIVATE

USE AND ENTER ONLY SECURE WEBSITES

USE STRONG PASSWORDS FOR ALL YOUR ACCOUNTS

DO NOT OPEN ATTACHMENTS IN SPAM EMAILS

DO NOT GIVE BANK ACCOUNT DETAILS TO UNKNOWN PEOPLE

BE ALERT WHILE USING PUBLIC WIFI HOTSPOTS

GOLDEN RULES TO FOLLOW ONLINE !

DO NOT GIVE OUT PERSONAL INFORMATION.

DO NOT SHARE INAPPROPRIATE PICTURES WITH ANYONE.

REMEMBER NOT EVERYONE ONLINE IS WHO THEY SAY THEY ARE.

AVOID OPENING EMAILS OR ATTACHMENTS FROM STRANGERS.

DO NOT REACT WHEN CYBER BULLIED INSTEAD BLOCK, KEEP A RECORD AND REPORT IT.

NEVER ARRANGE TO MEET SOMEONE IN PERSON WHOM YOU'VE MET ONLINE.

THANK YOU