## 1. Cyber Crime (सायबर गुन्हेगारी)

इंटरनेटच्या माध्यमातून इलेक्ट्रोनिक्स उपकरणे उदा. संगणक, लॅपटॉप, मोबाईल इ. साधनांचा वापर करून केले जाणारे गुन्हेगारी कृत्य म्हणजे सायबर गुन्हेगारी होय.

## 2. Cyber Criminals (सायबर गुन्हेगार)

संगणक क्षेत्रातील तांत्रिक ज्ञान असणारी व्यक्ती अथवा व्यक्तींचा समूह जे आपल्या ज्ञानाचा वापर इंटरनेटच्या माध्यमातून गुन्हेगारी कृत्य करण्यासाठी करतात त्यांना सायबर गुन्हेगार म्हणतात.

## 3. Cyber Crime Victims (सायबर गुन्हेगारीचे बळी)

फसवली गेलेली व्यक्ती, व्यक्तींचा समूह अथवा एखादी संस्था ज्यांचे नुकसान सायबर गुन्ह्यामुळे होते, त्यांना सायबर गुन्हेगारीचे बळी असे संबोधले जाते.

## 4. सायबर क्राइम करण्यामागील सायबर गुन्हेगारांचे उद्देश

सायबर क्राइमचा मुख्य उद्देश हा सहज व जलद पद्धतीने पैसे मिळवणे असतो. तसेच संगणक, मोबाईल यांमधील वैयक्तिक माहिती (Data) इंटरनेटच्या माध्यमातून चोरणे हा देखील एक उद्देश असतो.

## 5. सायबर हल्ला होण्यामागील कारणे

1. वाढते डिजिटलीकरण व वाढता इंटरनेटचा वापर.
2. इंटरनेटच्या माध्यमातून ओळख लपविण्याची असणारी संधी.
3. दुरून हल्ला करण्याची असणारी सोय.
4. इंटरनेटच्या माध्यमातून होणाऱ्या आर्थिक व्यवहारांमध्ये वाढ.
5. द्रुतगतीने वाढणाऱ्या ऑनलाइन सेवा.
6. सायबर गुन्हेगारीबाबत समाजात असणारी अपुरी जागरूकता.

## 6. सोशल मीडिया

प्रत्येक माणूस आपल्या भावना व्यक्त करण्यासाठी सोशल मीडियाचा वापर करत असतो. समाजातील प्रत्येक व्यक्ती सोशल मीडियावर टाकत असणाऱ्या पोस्ट अथवा माहितीचे अवलोकन हे सायबर गुन्हेगार व जिल्हा स्तरांवर असणारे सायबर पोलीस करत असतात.

आपण सोशल मीडियावर टाकलेल्या माहितीचे अवलोकन करून सायबर गुन्हे कोणासोबत करावयाचा हे सायबर गुन्हेगार ठरवित असतात. त्यामुळे आपल्यासोबत कोणताही सायबर गुन्हा घडू नये असे वाटत असेल तर आपण सोशल मीडियावर आपल्याकडे असणारी अति संवेदनशील, आर्थिक, वैयक्तिक, गोपनीय व महत्त्वपूर्ण माहिती सोशल मीडियावर टाकू नये. तसेच सोशल मीडियावर माहिती टाकत असताना आपले वयक्तिक व सोशल जीवनशैली यामध्ये फरक ठेऊन त्यामध्ये कोणत्याही पद्धतीची सरमिसळ करू नये. तसेच कोणतीही खोटी माहिती, अफवा, कोणाची बदनामी होईल असा मजकूर समाजामध्ये तेढ निर्माण करणारे मेसेज अथवा अश्लील आशयाचे मेसेज पाठवू नयेत. ही कृत्ये केल्यास आपल्याकडून सायबर गुन्हे घडतील की जे माहिती तंत्रज्ञान कायदा 2000 अंतर्गत कारवाईस पात्र ठरतील. आपण याची दक्षता घ्यावी.

## 7. सायबर गुन्हेगारीचे प्रकार

I. **हॅकिंग**

हॅकिंग म्हणजे दुसऱ्याच्या संगणक अथवा मोबाईल प्रणालीमध्ये अनधिकृत प्रवेश मिळविणे होय.

II. **फिशिंग**

फिशिंग या सायबर गुन्हेगारी प्रकारामध्ये सायबर गुन्हेगार हे सायबर क्राइम ज्या सोबत करायचा आहे अशा व्यक्तीच्या भीती, उस्तुकता, लोभ, अश्लिल साहित्य अशा भावनांशी खेळ करुन खोट्या सवांदप्रणालींचा (वेबसाईट्स, ई-मेल, लिंक अथवा बनावट संदेश) वापर करुन त्यांच्याकडे असणाऱ्या पैसे अथवा वैयक्तिक, संवेदनशील, महत्त्वपूर्ण, गोपनीय माहितीची चोरी करतात.

III. **पासवर्ड हॅकिंग/अटॅक**

आपल्या संगणक अथवा मोबाईल प्रणालीसाठी वापरल्या जाणाऱ्या पासवर्ड, पिन यांची चोरी करणे.

IV. **स्पूफिंग**

या प्रकारामध्ये सायबर गुन्हेगार हे दुसऱ्या व्यक्तीची ओळख, आवाज अथवा फोटो, व्हिडिओचा वापर करून खोटी ओळख निर्माण करतात. लोकांचा विश्वास संपादन करून त्यांच्याकडून पैसे, वैयक्तिक, संवेदनशील, महत्त्वपूर्ण माहितीची चोरी करतात.

v. **मॅलेशीयस कोड (Malicious Code)**

**मॅलेशीयस कोड म्हणजे सायबर गुन्हेगारांनी वाईट हेतूने प्रेरित होऊन तयार केलेला सॉफ्टवेअर प्रोग्राम किंवा कोड होय ज्याला व्हायरस असे संबोधले जाते. अशा प्रकारचे सॉफ्टवेअर प्रोग्राम संगणक अथवा मोबाईल प्रणालीमध्ये दुरून आणि गुप्तपणे प्रवेश करून त्यावरील माहितीची चोरी करणे अथवा त्याची नासधूस करणे यासाठी वापरले जातात.**

## 8. सायबर सुरक्षा (Cyber Security)

**सायबर सुरक्षा म्हणजे संगणक अथवा मोबाईल जे इंटरनेटसोबत नेटवर्कमध्ये अथवा स्वतंत्र जोडलेले असताना त्यावरील सॉफ्टवेअर, डेटा व इतर सेवा यांना अनधिकृत प्रवेशापासून व सायबर हल्ल्यांपासून सुरक्षित ठेवणे. या प्रक्रियेला सायबर सुरक्षा असे म्हणतात.**

## 9. सायबर सुरक्षिततेसाठी बँकांच्या ग्राहकांनी करावयाच्या गोष्टी (What to do's)

A) इंटरनेट बँकिंग सुविधा वापरण्यापूर्वी वापरत असलेली वेबसाईट ही बँकेचीच आहे याची खात्री करावी व नंतरच लॉगिन क्रेडेन्शियल्स व पासवर्ड टाकावेत.

B) बँकेकडून येणाऱ्या ई-मेलमधील बँकेच्या लोगोवर विश्वास ठेवू नये. मेल बँकेकडून आला आहे याची खात्री केल्याशिवाय उघडू नये.

C) बँकेचे मोबाईल बँकिंग ॲप हे डाउनलोड करताना Google Play Store अथवा अधिकृत ठिकाणाहूनच डाउनलोड करावे.

D) सोशल मीडिया अकाउंट अथवा ई-मेल अकाउंटसाठी मल्टी-फॅक्टर ऑथेंटिकेशनचा वापर करावा.

E) WhatsApp अथवा E-mail द्वारे येणाऱ्या Malicious Link वर क्लिक करू नये.

F) मोबाईलवर लायसन्स antivirus सॉफ्टवेअर वापरावेत.

G) बँकेकडून येणारे मेसेजस, ई-मेलची त्वरित पाहणी करावी व आपल्या बँकेच्या खात्याचे वारंवार अवलोकन करावे.

H) आपल्या मोबाईलवरून मोबाइल बँकिंग ॲप, यूपीआय, इंटरनेट बँकिंग ॲप, सार्वजनिक ठिकाणी वापरताना योग्य ती खबरदारी घ्यावी.

I) आपल्या बँक खाते (डिटेल्स) अथवा त्याच्याशी संबंधित इतर संवेदनशील माहिती उदा. पिन, पासवर्ड इत्यादी गोष्टी मोबाईलवर साठवून ठेवू नये.

J) आपण वापरत असलेले मोबाईल ॲप (लेटेस्ट/मोस्ट रिसेंट व्हर्जनला अपडेटेड असल्याची खात्री करावी) अथवा इंटरनेट बँकिंग सेवा वापरत असाल तर इंटरनेट/सुरक्षा संबंधित प्रणाली नेहमी अद्ययावत (Updated) अवस्थेत ठेवावी.

K) आपण इंटरनेट बँकिंग अथवा मोबाइल बँकिंगसाठी वापरत असलेला संगणक, लॅपटॉप, मोबाईलची ऑपरेटिंग सिस्टीम वारंवार अपडेट/अप टू डेट ठेवावी.

L) आपले ATM कार्ड हे दुसऱ्या कोणाच्या हाती लागू देऊ नये. तसेच आपल्या ATM, UPI App चा पिन हा दुसऱ्या कोणालाही सांगू नये, कोणासमोर टाकू नये, कोठेही लिहून ठेवू नये.

M) आपल्याला येणारा SMS द्वारे किंवा E-Mail द्वारे येणारा One Time Password (OTP) कोणाला सांगू नये अथवा शेअर करू नये.

N) आपल्या मोबाईलवर बँकेकडून येणारा फोन जर 1600xxxxxx या नंबरवरून येत असल्यास तो फोन call अधिकृत समजावा व या नंबर व्यतिरिक्त बँकेच्या नावाखाली येणारे इतर calls fraud समजावेत.

O) बँक कधीही आपल्याकडे आपली संवेदनशील माहिती उदा. OTP, PIN, Password व इतर PII माहिती उदा. आधार कार्ड, पॅनकार्ड नंबर कधीही मागत नाही. त्यामुळे फोन अथवा ई-मेलद्वारे माहिती कोणासही शेअर करू नये.

P) मोबाईल बँकिंग ॲप अथवा इंटरनेट बँकिंग ॲप वापरताना नेहमी अधिकृत इंटरनेट कनेक्शनचा वापर करावा.

Q) आपण किचकट (Complex) स्वरूपाचा Password किंवा PIN वापरावा. तो दर २१ दिवसांनी वारंवार बदलावा. पूर्वी वापरलेला Password किंवा PIN परत वापरू नये.

R) आपल्या संगणकावर अथवा मोबाईलवर अनधिकृत किंवा Pirated Software वापरू नये.

S) कोणत्याही आमिषाला अथवा प्रलोभनाला बळी न पडता जागरूक राहणे आवश्यक आहे.

## <u>10. खालील गोष्टी सायबर सुरक्षतेच्या अनुषंगाने करू नयेत (What Not to Do)</u>

A) बँकेच्या नावाखाली व बँकेचे प्रतिनिधी बोलत आहे असे सांगून तुमच्याकडून तुमचा पासवर्ड, पिन नंबर, क्रेडिट/डेबिट कार्ड डिटेल्स किंवा इतर माहिती विचारणाऱ्या कोणत्याही फोन अथवा ई-मेलला प्रतिसाद देऊ नये.

B) इंटरनेट बँकिंग अथवा मोबाईल बँकिंग सुविधेचा वापर करताना ओपन / पब्लिक Wi-Fi अथवा इंटरनेट कनेक्शनचा वापर करू नये.

C) आपल्या कामकाजाच्या ठिकाणी वापरत असणारा ई-मेल एड्रेसेस सार्वजनिक ठिकाणी उदारणार्थ ई-कॉमर्स वेबसाईट, रिवार्ड vouchers, ब्लॉग्ज इ. ठिकाणी

वापरू नये कारण हॅकर्स कडून त्या ई-मेलचा वापर सायबर  अटॅक साठी होऊ शकतो.

D) आपली ई-मेल एड्रेसेसवर किंवा SMS द्वारे येणाऱ्या संदेशांमधील संशयास्पद किंवा अनोळखी मेलवर (मेल ओपनकरू नये) किंवा SMS मधील लिंकवर क्लिक करू नये.

E) आपल्याकडील लॉगिन क्रेडन्शिअल्स/पासवर्ड, OTP, UPI PIN, ATM PIN, PII इ. गोष्टी कोणत्याही व्यक्तीबरोबर शेअर करू नयेत आणि कोणत्याही कागदावर लिहून ठेऊ नयेत.

F) आपला मोबाईल फोन किंवा लॅपटॉप कोणत्याही अनोळखी व्यक्तीच्या ताब्यात देऊ नये. तसेच आपल्याकडे असणाऱ्या संवेदनशील, गोपनीय व महत्त्वपूर्ण माहितीची सार्वजनिक ठिकाणी चर्चा करू नये.

G) कॉलर आयडी मार्फत येणारे Call/SMS किंवा Mail हे अधिकृत आहेत असे समजून त्यावर विश्वास ठेवू नये, कारण त्यामध्ये स्पूफिंग attack होण्याची शक्यता असते.

H) आपली जन्मतारीख, पत्ता, टोपणनाव, दूरध्वनी क्रमांक इत्यादी वैयक्तिक माहिती सोशल मीडियावर शेअर करू नये. कारण गुन्हेगार या माहितीचा वापर करून आपल्या संपत्ती व सुरक्षिततेला धोका निर्माण करू शकतात/सायबर हल्ला होण्याची शक्यता असते.

जर आपल्या सोबत सायबर हल्ल्याद्वारे फसवणूक झाली (सायबर हल्ला) झाला तर :

- त्वरित (नोंदणीकृत मोबाईल वरून) 1930 या हेल्पलाइन क्रमांकावर संपर्क साधावा/तक्रार नोंदवावी.
- अथवा https://www.cybercrime.gov.in (National Cyber Crime Reporting Portal) येथे तक्रार नोंदवावी.
- अथवा स्थानिक जिल्हा सायबर पोलीस स्टेशनमध्ये तक्रार नोंदवावी.