**मोबाइल वापरातील सायबर धोके.**

• मोबाईल फिशिंग

संगणकावर ज्याप्रमाणे फिशिंग केले जाते, तसेच फिशिंग ऍटॅक मोबाईल वापरकर्त्यांवरसुद्धा होऊ शकतात. इथेही इमेल आणि मेसेजेसद्वारे ग्राहकांचा विश्वास संपादन करून खाजगी माहिती मिळवण्याचा प्रयत्न केला जातो.

याप्रकारात सामान्यत: गुगल प्ले स्टोअर सोडून इतर एखाद्या वेबसाईटवरून व्हिडिओ प्लेअरच्या नावाखाली खोटे सॉफ्टवेअर्स डाऊनलोड करण्यास ग्राहकांना भाग पाडले जाते.

• व्हायरसची लागण झालेल्या मोबाईलपासून आजूबाजूच्या मोबाईलना धोका उत्पन्न होणे

एक संक्रमित मोबाइल डिव्हाइस आपण संस्थेच्या परिमिती मोडण्यासाठी आणि थेट त्याऐवजी आपण आधीच थेट नेटवर्क प्रवेश मिळाला आहे म्हणून, इतर काही खंडित करण्यात येत नेटवर्कवर डिव्हाइसेस हल्ला करण्यास अनुमती देते.

तुम्हीच तुमचे शत्रू होऊ शकाल कारण..

* तुम्ही जितकी अधिकाधिक खाजगी आणि संवेदनशील माहिती (पासवर्ड्स, खाजगी फोटोज) तुमच्या मोबाईलमध्ये साठवाल, तितकेच ते अधिकाअधिक धिओकादायक होईल.
* मोबाईलमध्ये चांगले ऍंटिव्हायरस सॉफ्टवेअर इन्स्टॉल करा आणि ते वेळोवेळी अपडेट करा.

**कसे टाळण्यासाठी.**

* आपल्या संगणक/मोबाईलवरील माहितीचा नेहमी बॅक अप ठेवा
* आपल्या इमेल किंवा SMS मध्ये आलेल्या कोणत्याही दुव्यांवर क्लिक करण्यापूर्वी तीनदा विचार करा.
* नेहमी आपला डेटा बॅक अप ठेवा
* तुमच्या मोबाईलचे सिक्यिरिटी फिचर्स जाणून घ्या आणि त्यांचा वापर करा.
* अकारण आपला मोबाईल नंबर कुठेही देऊ नका.
* ओपन आणि फुकट उपलब्ध असलेले वाय-फाय कनेक्शन वापरताना काळजी घ्या. थोडाही संशय आल्यास असे कनेक्शन वापरू नका.

