**सायबर विश्वातील धोके**

 **सामाजिक अभियांत्रिकी (सोशल इंजिनिअरिंग)**

फिशिंग

* फिशिंग या सायबर गुन्ह्याच्या प्रकारात इमेलचा वापर करणार्‍या लोकांना खरे वाटतील असे खोटे इमेल्स पाठवण्यात येतात. हे इमेल्समधून बँका किंवा जिथे आपले खाते असू शकते अशा वित्तीय संस्थांकडून आले आहेत असे भासवले जाते.
* ग्राहकांना आर्थिकदृष्ट्या लुबाडणे हे फिशिंगचे मुख्य ध्येय आहे. यामध्ये हॅकर वापरकर्त्याची संवेदनशील माहिती उदा. युझर आयडी-पासवर्ड, क्रेडिट कार्डावरील सीव्हीव्ही नंबर, मोबाईलवरती येणारा वन टाईम पासवर्ड(OTP) इत्यादी चलाखीने मिळवली जाते.

फिशिंगचे प्रकार

ईमेलद्वारे फिशिंग:

* तुमच्या ओळखीचे लोक परदेशात अडचणीत आहेत किंवा अडकले आहेत असा खोटा दावा करणारे इमेल्स.
* नामांकित आणि विश्वसनीय संस्थांच्या नावाखाली खोट्या वेबसाईटच्या लिंक्स तयार करून लोकांना इमेल्समधून पाठवून लोकांना त्या लिंक्सवर क्लिक करण्यास भाग पाडणे.
* धमक्या (उदा. तुमच्या संगणकावरील माहिती लॉक करणे) देणारे इमेल्स पाठवणे.
* लोकांनी न पाठवलेल्या तक्रारी स्वीकृत करणारे इमेल्स त्यांना पाठवून त्या इमेल्समधील लिंकवर क्लिक करण्यास भाग पाडणे.

Spear फिशिंग

* Spear फिशिंग हे नेहमीच्या फिशिंगपेक्षा थोडेसे वेगळे असते. यामधले हल्ले अधिक व्यक्तिगत स्वरूपाचे असतात. त्यामुळे ग्राहकांच्या फसवणूकीचे प्रमाण यामध्ये अधिक असते.
* Spear फिशिंग करण्यापूर्वी हॅकर ग्राहकाची सार्वजनिकरित्या उपलब्ध असलेली माहिती मिळवतात. या माहितीच्या आधारे ते ग्राहकाची बनावट व्यक्तिरेखा बनवून त्याच्या मित्र, नातेवाईक आणि इतर विश्वासून संबंधितांना फसवतात.

Vishing

* **विशिंग म्हणजे Voice वापरून केलेले फिशिंग. यामध्ये ग्राहकांना फोन करून त्यांची खाजगी माहिती मिळवली जाते. या माहितीचा तोतयेगिरी करण्यासाठी म्हणजेच खोटी ओळख तयार करण्यासाठी वापरली जाते.**.
* या प्रकारात फसवणूक करणारी व्यक्ती जणू काही कायदेशीर संस्थेच्या वतीने बोलत असल्याचे भासवून ग्राहकाने आपली खाजगी माहिती दिल्यास त्याचा फायदा होईल असा विचार करायला भाग पाडते.
* फोन करणारी व्यक्ती आपण बँक, बिल्डिंग सोसायटी, सरकारी संस्था किंवा कुणी खरोखरीचा व्यावसायिक असल्याचे भासवतात आणि आपल्या संभाषणचातुर्याने ग्राहकाची खाजगी माहिती काढून घेतात.

Smishing

* Smishing या प्रकारात ग्राहकाला त्याच्या मोबाईलवर एखादा व्हायरस किंवा एखादे धोकादायक सॉफ्टवेअर डाऊनलोड करायवयास भाग पाडले जाते.
* नागSmishing म्हणजे थोडक्यात, "एसएमएस फिशिंग." स्मिशिंगमध्ये ग्राहकाला SMS पाठवून त्यांना उत्तरादाखल त्यांची खाजगी माहिती SMS करण्यास उद्युक्त केले जाते. ज्या नंबरवरून असे मेसेजेस येतात, ते सहसा प्रीमियम-रेट नंबर असतात आणि त्यांना उत्तर दिल्यानंतर ग्राहकास मोठे बिल येऊ शकते

 **सोशल इंजिनिअरिंग कसे टाळाल?**

• आपली खाजगी माहिती कुणालाही देऊ नका.

• आलेल्या माहितीची प्रथम खातरजमा करा आणि मगच उत्तर द्यायचे की नाही ते ठरवा.

• कोणतीही फाईल , सॉफ्टवेअर किंवा ऍप डाउनलोड करताना सावध रहा.

• कितीही आकर्षक असल्या तरी परदेशी ऑफर स्वीकारू नका.

• तुमचे मोबाईल्स आणि संगणकावर ऍंटीव्हायरस इन्स्टॉल करा आणि ते अद्ययावत ठेवा.

• इतरांना सहज अंदाज बांधता येतील असे पासवर्ड्स (ऊदा. वाढदिवस, प्रियजनांची नावे) ठेवू नका आणि काही महिन्यांनंतर ते बदलण्याची दक्षता घ्या.

• कुठलीही माहिती इंटरनेटवर शेअर करताना काळजी घ्या.

* आपल्या संगणक/मोबाईलवरील माहितीचा नेहमी बॅक अप ठेवा
* आपल्या इमेल किंवा SMS मध्ये आलेल्या कोणत्याही दुव्यांवर क्लिक करण्यापूर्वी तीनदा विचार करा.