कसरी हुन्छ इन्टरनेट ह्याकिङ ?

एउटा क्लिकदेखि डिजिटल साम्राज्य कब्जासम्म



एजेन्सी

इन्टरनेटले संसारलाई एउटा सानो गाउँजस्तै बनाएको छ। केही सेकेन्डमै संसारको जुनसुकै कुनामा सन्देश पठाउन, आर्थिक कारोबार गर्न, सूचना आदानप्रदान गर्न र सरकारी सेवा लिन सकिन्छ। तर यही सुविधासँगै अर्को अदृश्य जोखिम पनि बढिरहेको छ। त्यो हो - इन्टरनेट ह्याकिङ। हामीले दैनिक प्रयोग गर्ने मोबाइल, कम्प्युटर, सामाजिक सञ्जाल, इमेल, बैंकिङ एप र सरकारी वेबसाइटसमेत साइबर आक्रमणको निशानामा पर्न सक्छन्।

धेरैलाई ह्याकिङ भन्नासाथ कुनै व्यक्तिले कम्प्युटरको पर्दामा जटिल संकेत र कोड चलाएर अर्को व्यक्तिको उपकरण नियन्त्रणमा लिएको दृश्य सम्झना आउँछ। तर वास्तविकता त्यसभन्दा फरक र व्यापक छ। कतिपय अवस्थामा एउटा नक्कली इमेल खोल्नु, अपरिचित लिंकमा क्लिक गर्नु वा कमजोर पासवर्ड राख्नु नै साइबर अपराधीलाई प्रणालीभित्र प्रवेश गर्ने बाटो बन्न सक्छ।

ह्याकिङको मुख्य उद्देश्य कम्प्युटर वा नेटवर्कको सुरक्षा कमजोरी पहिचान गरी त्यसमा अनधिकृत पहुँच बनाउनु हो। सबै ह्याकिङ गैरकानुनी हुँदैनन्। प्रणालीको सुरक्षा परीक्षण गर्न अनुमति लिएर गरिने ह्याकिङलाई नैतिक ह्याकिङ भनिन्छ। तर अनुमति नलिई अरूको सूचना चोर्ने, प्रणाली नियन्त्रणमा लिने, आर्थिक क्षति पुऱ्याउने वा सेवा अवरुद्ध गर्ने गतिविधि साइबर अपराध हुन्।

एउटा क्लिकबाट सुरु हुन सक्छ आक्रमण

इन्टरनेट ह्याकिङको सबैभन्दा प्रचलित माध्यममध्ये एक हो - फिसिङ। यसमा साइबर अपराधीले प्रयोगकर्तालाई झुक्याएर गोप्य विवरण प्राप्त गर्ने प्रयास गर्छन्।

उदाहरणका लागि, कुनै व्यक्तिको इमेलमा बैंकको नाम र लोगो प्रयोग गरिएको सन्देश आउन सक्छ। उक्त सन्देशमा खातामा समस्या देखिएको भन्दै एउटा लिंक खोल्न भनिन्छ। प्रयोगकर्ताले त्यसलाई वास्तविक बैंकको सन्देश ठानेर लिंक खोल्छ र आफ्नो प्रयोगकर्ता नाम तथा पासवर्ड राख्छ। तर त्यो बैंकको वास्तविक वेबसाइट नभई अपराधीले तयार पारेको नक्कली वेबसाइट हुन सक्छ।

यसरी प्रयोगकर्ताले आफैँ उपलब्ध गराएको विवरण अपराधीको हातमा पुग्छ। त्यसपछि उनीहरूले बैंकिङ खाता, सामाजिक सञ्जाल वा इमेलमा अनधिकृत पहुँच बनाउने प्रयास गर्न सक्छन्।

फिसिङ इमेलमा मात्र सीमित छैन। एसएमएस, सामाजिक सञ्जालका सन्देश, फोन कल र नक्कली वेबसाइटमार्फत पनि यस्तो आक्रमण हुन सक्छ। यसलाई सामाजिक इन्जिनियरिङ भनिन्छ। यसको विशेषता भनेको प्रविधिको कमजोरीभन्दा मानिसको विश्वास, डर, जिज्ञासा वा हतारको फाइदा उठाउनु हो।

पासवर्ड कसरी चोरी हुन्छ ?

पासवर्ड डिजिटल सुरक्षाको पहिलो ढोका हो। तर धेरै प्रयोगकर्ताले सजिलो सम्झन सकिने नाम, जन्ममिति, मोबाइल नम्बर वा सामान्य शब्दलाई पासवर्ड बनाउँछन्। एउटै पासवर्ड विभिन्न वेबसाइट र एपमा प्रयोग गर्ने प्रवृत्तिले जोखिम अझ बढाउँछ।

साइबर अपराधीले चोरी भएका पुराना पासवर्ड र प्रयोगकर्ता नामको सूची प्रयोग गरी अन्य वेबसाइटमा पनि लगइन प्रयास गर्न सक्छन्। एउटै पासवर्ड धेरै ठाउँमा प्रयोग गरिएको छ भने एउटा वेबसाइटबाट चोरी भएको विवरण अर्को खातासम्म पुग्न सक्छ। यसलाई क्रेडेन्सियल स्टफिङ भनिन्छ।

त्यस्तै, ब्रुट फोर्स आक्रमणमा स्वचालित प्रणालीले सम्भावित पासवर्डहरू बारम्बार परीक्षण गर्छ। कमजोर र छोटा पासवर्ड यस्तो आक्रमणबाट सजिलै जोखिममा पर्न सक्छन्।पासवर्ड चोरीको अर्को माध्यम मालवेयर हो। यो कम्प्युटर वा मोबाइलमा प्रवेश गर्ने हानिकारक सफ्टवेयर हो। यसले प्रयोगकर्ताका गतिविधि निगरानी गर्ने, गोप्य विवरण संकलन गर्ने वा उपकरणमा रहेका फाइलमा पहुँच बनाउने काम गर्न सक्छ।

भाइरस र मालवेयरबाट कसरी हुन्छ ह्याकिङ ?

कम्प्युटर भाइरस, ट्रोजन, स्पाइवेयर र च्यान्समवेयर मालवेयरका विभिन्न प्रकार हुन्।

भाइरसले आफूलाई अन्य फाइल वा प्रोग्रामसँग जोडेर फैलिन सक्छ। ट्रोजन उपयोगी सफ्टवेयरजस्तो देखिएर प्रयोगकर्तालाई झुक्याउँदै उपकरणमा प्रवेश गर्छ। स्पाइवेयरले प्रयोगकर्ताको गतिविधि निगरानी गरी सूचना संकलन गर्न सक्छ।

च्यान्समवेयर भनेको उपकरण वा नेटवर्कमा रहेका फाइललाई लक अथवा इन्क्रिप्ट गरेर खोल्न नसकिने बनाउने हानिकारक सफ्टवेयर हो। त्यसपछि अपराधीले फाइल फिर्ता उपलब्ध गराउन रकम माग्न सक्छन्।

यस्ता सफ्टवेयर नक्कली एप, संक्रमित फाइल, असुरक्षित वेबसाइट, इमेलको संलग्न फाइल वा कमजोर सुरक्षा प्रणालीमार्फत उपकरणमा पुग्न सक्छन्।

कतिपय अवस्थामा प्रयोगकर्ताले पाइरेटेड सफ्टवेयर वा अनधिकृत वेबसाइटबाट डाउनलोड गरेको फाइलमा मालवेयर लुकेको हुन्छ। त्यसैले नचिनेको स्रोतबाट सफ्टवेयर डाउनलोड गर्नु जोखिमपूर्ण मानिन्छ।

वेबसाइट र सरकारी प्रणाली कसरी ह्याक हुन्छन् ?

व्यक्तिगत खाता मात्र होइन, वेबसाइट, बैंक, अस्पताल, सञ्चार संस्था र सरकारी निकायका प्रणाली पनि साइबर आक्रमणको निशानामा पर्न सक्छन्।

वेबसाइट निर्माण गर्दा प्रयोग गरिएको सफ्टवेयर पुरानो हुनु, सुरक्षा अपडेट नगर्नु, कमजोर पासवर्ड राख्नु वा गलत तरिकाले प्रणाली सञ्चालन गर्नु आक्रमणकारीका लागि अवसर बन्न सक्छ।

उदाहरणका लागि, कुनै वेबसाइटमा प्रयोगकर्ताले सूचना राख्ने स्थानमा सुरक्षा कमजोरी छ भने आक्रमणकारीले त्यसको दुरुपयोग गरेर डेटाबेसमा अनधिकृत पहुँच बनाउने प्रयास गर्न सक्छन्। एसक्युएल इन्जेक्सन भनिने आक्रमण यही प्रकृतिको हो।त्यस्तै, क्रस साइट स्क्रिप्टिङ अर्थात् एक्सएसएसमार्फत वेबसाइटमा हानिकारक स्क्रिप्ट चल्न सक्ने कमजोरीको दुरुपयोग गरिन्छ। यसबाट प्रयोगकर्ताको ब्राउजर वा वेबसाइटको सुरक्षामा असर पर्न सक्छ।

डिस्ट्रिब्युटेड डिनायल अफ सर्भिस अर्थात् डिडस आक्रमणमा ठुलो संख्यामा उपकरणबाट एउटै वेबसाइट वा सर्भरमा अत्यधिक अनुरोध पठाइन्छ। त्यसले गर्दा वास्तविक प्रयोगकर्ताले वेबसाइट खोल्न नसक्ने अवस्था आउन सक्छ।

यसरी वेबसाइटको सूचना चोरी नभए पनि सेवा अवरुद्ध हुन सक्छ। सरकारी वेबसाइट, बैंकिङ प्रणाली र अनलाइन सेवा प्रदायक संस्थाका लागि यस्तो आक्रमण गम्भीर चुनौती बन्न सक्छ।

> पासवर्ड चोरी, नक्कली वेबसाइट, कमजोर सुरक्षा प्रणाली र मानवीय त्रुटि ह्याकिङका प्रमुख माध्यम; व्यक्तिगत विवरणदेखि बैंकिङ प्रणाली र राष्ट्रिय सुरक्षा संरचनासम्म जोखिम

वाइफाइबाट पनि हुन सक्छ साइबर आक्रमण

सार्वजनिक स्थानमा उपलब्ध निःशुल्क वाइफाइ प्रयोग गर्दा पनि सावधानी आवश्यक हुन्छ। होटल, विमानस्थल, क्याफे र सार्वजनिक स्थलमा उपलब्ध वाइफाइ नेटवर्कको नाम नक्कली बनाएर प्रयोगकर्तालाई जोडिन प्रलोभन दिन सकिन्छ।

कतिपय अवस्थामा आक्रमणकारीले प्रयोगकर्ता र वास्तविक वेबसाइटबीचको सञ्चारमा हस्तक्षेप गर्ने प्रयास गर्छन्। यसलाई म्यान इन द मिडल आक्रमण भनिन्छ।

यस्तो अवस्थामा प्रयोगकर्ताले पठाएको वा प्राप्त गरेको सूचना असुरक्षित हुन सक्छ। विशेषगरी इन्क्रिप्सन नभएका वेबसाइट वा असुरक्षित नेटवर्क प्रयोग गर्दा जोखिम बढ्न सक्छ।

त्यसैले सार्वजनिक वाइफाइ प्रयोग गर्दा बैंकिङ कारोबार, संवेदनशील सूचना आदानप्रदान र महत्त्वपूर्ण खातामा लगइन गर्ने काममा विशेष सतर्कता अपनाउनुपर्छ।

मोबाइल फोन पनि सुरक्षित छैनन्

स्मार्टफोनमा व्यक्तिगत तस्बिर, सम्पर्क नम्बर, बैंकिङ विवरण, इमेल, सामाजिक सञ्जाल र अन्य महत्त्वपूर्ण सूचना हुन्छन्। यही कारण मोबाइल फोन साइबर अपराधीको आकर्षणको केन्द्र बनेका छन्।

नक्कली मोबाइल एप, असुरक्षित लिंक, संक्रमित फाइल र अनावश्यक अनुमति माग्ने एपमार्फत मोबाइलमा मालवेयर प्रवेश गर्न सक्छ।

कुनै एपले आफ्नो कामसँग सम्बन्ध नभएका अत्यधिक अनुमति माग्छ भने त्यसले प्रयोगकर्ताको गोपनीयतामा जोखिम सिर्जना गर्न सक्छ। उदाहरणका लागि, सामान्य क्याल्कुलेटर एपले सम्पर्क सूची, माइक्रोफोन वा सन्देशमा पहुँच माग्नु शंकास्पद हुन सक्छ।

मोबाइलको अपरेटिङ सिस्टम र एप नियमित अपडेट नगर्दा पुराना सुरक्षा कमजोरीको दुरुपयोग हुन सक्ने सम्भावना रहन्छ।

ह्याकिङबाट कसरी बच्ने ?

साइबर आक्रमण पूर्णरूपमा रोक्न कठिन भए पनि सावधानी अपनाएर जोखिम निकै कम गर्न सकिन्छ। यसका लागि व्यक्तिगत प्रयोगकर्ता, संस्था र सरकारी निकाय सबैले डिजिटल सुरक्षालाई प्राथमिकता दिनुपर्छ।

सबैभन्दा पहिले, प्रत्येक खाताका लागि फरक र बलियो पासवर्ड प्रयोग गर्नुपर्छ। पासवर्ड व्यवस्थापन गर्न पासवर्ड म्यानेजर उपयोगी हुन सक्छ। सम्भव भएसम्म २ चरणको प्रमाणीकरण अर्थात् टु फ्याक्टर अथेन्टिकेसन सक्रिय गर्नुपर्छ।

अपरिचित इमेल, सन्देश वा सामाजिक सञ्जालमा आएको लिंक खोल्नुअघि त्यसको स्रोत जाँच गर्नुपर्छ। बैंक वा सरकारी निकायको नाममा आएको सन्देशमा गोप्य विवरण मागिएको छ भने सम्बन्धित संस्थाको आधिकारिक माध्यमबाट पुष्टि गर्नुपर्छ। मोबाइल र कम्प्युटरमा नियमित सुरक्षा अपडेट गर्नुपर्छ। आधिकारिक एप स्टोरबाट मात्र एप डाउनलोड गर्ने, अनावश्यक एप हटाउने र महत्त्वपूर्ण फाइलको सुरक्षित ब्याकअप राख्ने बानी बसाल्नुपर्छ।

संस्थाहरूले पनि नियमित सुरक्षा परीक्षण, कर्मचारीलाई साइबर सुरक्षासम्बन्धी तालिम, पहुँच नियन्त्रण, नेटवर्क निगरानी र आकस्मिक पुनःस्थापना योजना बनाउन आवश्यक हुन्छ।

डिजिटल युगको नयाँ सुरक्षा चुनौती

ह्याकिङ अब व्यक्तिगत कम्प्युटर वा सामाजिक सञ्जालमा सीमित विषय रहेन। बैंकिङ, स्वास्थ्य, शिक्षा, ऊर्जा, सञ्चार, यातायात र सरकारी सेवा डिजिटल प्रणालीमा निर्भर हुँदै जाँदा साइबर सुरक्षाको महत्त्व पनि बढेको छ।

एउटा व्यक्तिको सामाजिक सञ्जाल खाता नियन्त्रणमा लिनेदेखि कुनै संस्थाको हजारौँ ग्राहकको विवरण चोरी गर्नेसम्म साइबर आक्रमणको दायरा फैलिएको छ। कतिपय आक्रमणले आर्थिक क्षति मात्र होइन, संस्थाको प्रतिष्ठा र सेवाको निरन्तरतामा समेत असर पार्न सक्छन्।यसको समाधान केवल महँगो प्रविधि खरिद गर्नु होइन। डिजिटल साक्षरता, नियमित सुरक्षा परीक्षण, कानुनी कार्यान्वयन र प्रयोगकर्ताको सचेतना पनि उत्तिकै आवश्यक छन्।

इन्टरनेट प्रयोग गर्नु आजको आवश्यकता बनिसकेको छ। तर डिजिटल संसारमा जोडिनु भनेको आफ्नो व्यक्तिगत तथा संस्थागत सूचना सुरक्षाको जिम्मेवारी पनि लिनु हो। साइबर अपराधीले सधैँ जटिल प्रविधि प्रयोग गर्छन् भन्ने छैन। कहिलेकाहीँ प्रयोगकर्ताको एउटा असावधानी नै उनीहरूका लागि पर्याप्त हुन्छ। त्यसैले इन्टरनेटमा सुरक्षित रहनुको पहिलो सर्त प्रविधिको प्रयोगसँगै जोखिमबारे सचेत हुनु हो।

Letang Municipality
Office of the Municipal Executive
Letang-3, Morang
Koshi Province, Nepal

Invitation for Sealed Quotation

Date of first Publication: 2026/11/24

S. No.	IFB No.	Particulars	Estimated Cost Including PS Exclusive of VAT & Contingency (NRs.)	Bid Security Amount (NRs.)	Cost of Bidding Document (NRs)	Bid/Bid security Validity Period (Days)	Last Date of Bids Submission	Time for completion
1.	LM/MOR/SQ/G/2083-84/02	Supply of RCC Hume Pipe in Letang Municipality	1721987.00	50000.00	1000	45 days/ 75 days	2026/12/01, 12:00 Hours	2 months From Agreement
2.	LM/MOR/SQ/G/2083-84/03	Purchase of free medicines, surgical materials, and laboratory chemicals.	3925450.00	100000.00	1,000	45 days/ 75 days	2026/12/01, 12:00 Hours	2 months From Agreement

1. The Letang Municipality, Morang invites sealed quotations from registered Suppliers for the supply, delivery, and installation of Supply of RCC Hume Pipe in Letang Municipality.
2. The Letang Municipality, Morang invites sealed quotations from registered Suppliers for the supply, delivery, and installation of Purchase of free medicines, surgical materials, and laboratory chemicals.
3. Eligible Bidders may obtain further information and inspect the Sealed quotation Forms at the office of Letang Municipality, Morang at Letang, Morang or by reaching out to them at Telephone 021560666 or by dropping a mail at ito. letangmun@gmail.com or Visit web site https://letangmun.gov.np/

Chief Administrative Officer

गौरीगङ्गा नगरपालिका
नगर कार्यपालिकाको कार्यालय
चौमाला, कैलाली
सुदूरपश्चिम प्रदेश, नेपाल

सिलबन्दी प्राविधिक र आर्थिक प्रस्ताव पेश गर्ने सम्बन्धी सूचना

प्रथम पटक प्रकाशित मितिः २०८३/०८/०८

गौरीगङ्गा नगरपालिकाद्वारा विभिन्न फर्म/परामर्शदातासँग तपसिल बमोजिमका कार्य गर्नका लागी ToR/RFP बमोजिमका कागजात र सिलबन्दी प्राविधिक र आर्थिक प्रस्ताव पेश गर्न यो सूचना प्रकाशित गरिएको छ।

क्र. स.	प्रस्ताव नं.	विवरण	जम्मा रकम (मु.अ.क.सहित)	कैफियत
१	GGM/CS/ 02/2083/084	The Consulting Services for the preparation of Local Disaster and Climate Resilient Framework (LDCRF) of Gauriganga Municipality, Chaumala, Kailali	7,00,000/-	

१. सिलबन्दी प्राविधिक र आर्थिक प्रस्ताव पेश गर्नेले लिखित निवेदन सहित नविकरण भएको फर्म/ कम्पनी दर्ता प्रमाणपत्रको प्रतिलिपी, नविकरण भएको व्यवसाय दर्ता प्रमाणपत्रको प्रतिलिपी, मु.अ.क.दर्ता प्रमाणपत्रको प्रतिलिपी र आ.व. २०८२/०८३ को करचुक्ता वा म्याद थप प्रमाणपत्रको प्रतिलिपी संलग्न गरि पेश गर्नु पर्ने छ।

२. प्रस्ताव पेश गर्ने परामर्शदाताले कार्यालयमा अनिवार्य सुचिकृत गर्नुपर्ने छ। सुचिकृत नभएका निर्माण परामर्शदातालाई मूल्यांकन समावेश गर्न सकिने छैन। (नोटः तत्कालै सुचिकृत गरि प्रस्ताव पेश गर्न सकिनेछ)

३. BoQ मा आफुले कबोल गरेको रकम अंक र अक्षरमा स्पष्ट बुझिने गरि लेखेर पेश गर्नु पर्नेछ केरमेट भएको दररेट (BoQ) मुल्यांकनमा समावेश गरिने छैन।

४. ToR मा उल्लेख भए अनुसारका विज्ञहरुको CV र फर्मको कार्य अनुभव प्रमाणपत्र अनिवार्य रुपमा पेश गर्नु पर्नेछ। उक्त कार्यको लागी आवश्यक TOR/BOQ लगायत अन्य यस कार्यालयको वेवसाइटमा http://www.gaurigangamun.gov.np बाट डाउनलोड गर्न सकिनेछ।

५ उपरोक्त परामर्शको लागी सुचना प्रकाशित भएको मितिले १६ औं दिन दिउँसो १२:०० बजे भित्र कार्यालयमा शिलबन्दी गरि दुवै प्रस्ताव शिलबन्दी दर्ता गरी सक्नु पर्नेछ। रितपूर्वक दर्ता भएका दरभाउपत्रहरु सोही दिनको १:०० बजे गौरीगंगा नगरपालिकाको कार्यालयमा दरभाउपत्रदाताको रोहवरमा खोलिनेछ। दरभाउपत्रदाताको उपस्थिति नभएमा पनि दरभाउपत्र खोल्न वाधा पर्ने छैन।

६. यो सूचनामा उल्लेख हुन छुट भएका विषयहरु प्रचलित ऐन कानून वमोजिम हुनेछ। सो खरिद सम्वन्धि सम्पूर्ण अधिकार कार्यालयमा निहित रहनेछ।

प्रमुख प्रशासकीय अधिकृत

प्रभु बैंक लिमिटेड, शाखा कार्यालय आठबिसकोट, रुकुम (पश्चिम)का तपसिलमा उल्लेखित ऋणी तथा जमानतकर्तालाई कर्जा चुक्ता गर्ने तथा धितोमा रहेको सम्पत्ति, गोप्य शिलबन्दी बोलपत्र मार्फत लिलाम बिक्री गर्ने बारेको पुनः १५ दिने सार्वजनिक सूचना।

(सूचना प्रकाशित मिति २०८३/०८/०८ गते मंगलबारको सौर्य राष्ट्रिय दैनिक)

यस बैंक को तपसिलमा उल्लेखित ऋणीले विभिन्न शिर्षक अन्तरगत लिनुभएको ऋण कर्जा रकम चुक्ता भुक्तान गर्ने अवधी समाप्त भईसक्दा पनि बैंकसँग गर्नुभएको सम्झौता बमोजिम कर्जा चुक्ता फछ्र्यौट नगर्नु भएकोले यस बैंकबाट पटक पटक मौखिक तथा लिखित तरताकेता गर्दा समेत सोको पूर्ण बेवास्ता गरी ऋणी तथा जमानतकर्ताले कर्जा नियमित तथा चुक्ता फछ्र्यौट गर्ने तर्फ चासो नदेखाई आलटाल गरी बसेको हुँदा बैंकले कर्जा असुलीका लागि मिति २०८३/०२/१२ गते मंगलबारको सौर्य राष्ट्रिय दैनिक पत्रिकामा कर्जा चुक्ता गर्ने ३५ दिने सार्वजनीक सूचना तथा धितोमा रहेको सम्पत्ति गोप्य शिलबन्दी बोलपत्र मार्फत् लिलाम बिक्री गर्ने बारेको ७ दिने सार्वजनिक सूचना प्रकाशित गरिएकोमा सो सूचना बमोजिम कर्जा चुक्ता नभएको र धितो बापतको सम्पत्ती लिलाम बिक्री हुन नसकेकोले कर्जा असुलीका लागि कर्जा सुरक्षणको रुपमा बैंक समक्ष धितो रहेको तपसिलमा उल्लिखित सम्पत्ति जे जस्तो अवस्थामा छ सोही अवस्थामा गोप्य शिलवन्दी बोलपत्रको माध्यमवाट लिलाम बिक्री गरिने भएकोले उक्त सम्पत्ती के कति दर भाउ र मुल्यमा खरिद गरी लिने हो सो व्यहोरा खुलाई यो सूचना प्रकाशित भएको मितिले १५ (पन्ध्र) दिनभित्र गोप्य शिलबन्दी बोलपत्र बैंकको **शाखा कार्यालय, आठबिसकोट, रुकुम (पश्चिम)मा** दाखिल गर्नु हुन ईच्छुक व्यक्ति तथा संगठित संस्था सबैको जानकारीको लागि यो सूचना प्रकाशित गरिएको छ। प्राप्त बोलपत्रहरु यो सूचना प्रकाशित भएको मितिले १६ औं दिन अर्थात मिति २०८३/०८/२३ गते बुधबार (सो दिन सार्वजनिक विदा परेमा सोको लगत्तै बैंक खुलेको दिन) बैंकको **शाखा कार्यालय, आठबिसकोट, रुकुम (पश्चिम)मा** दिनको ठीक २:०० (दुई) बजे खोलिने भएकोले उक्त दिन उपस्थित हुन सम्बन्धित ऋणी, सुरक्षणधनी, ईच्छुक बोलपत्रदाता तथा सम्बद्ध सबैमा अनुरोध छ। प्राप्त बोलपत्रहरु बैंकले बिना कुनै कारण दर्शाई स्वीकार वा अस्वीकार गर्न सक्ने व्यहोरा समेत जानकारी गराईन्छ। पुनश्चः यो सूचना प्रकाशित भएको मितिले १५ पन्ध्र) दिन भित्र उक्त बांकी सम्पूर्ण कर्जाको साँवा ब्याज तथा हर्जाना लगायतका अन्य दै दस्तुर समेत तिरी बुझाई कर्जा चुक्ता फछ्र्यौट गर्न गराउनको लागि सम्बन्धित ऋणी, धितो सुरक्षण धनी तथा जमानतकर्ता समेतलाई यसै सूचनाद्धारा जानकारी गराईन्छ। उक्त म्याद भित्र समेत कर्जा चुक्ता नभएमा ऋणी तथा जमानतकर्ता लगायत नेपाल राष्ट्र बैंकको निर्देशन बमोजिम कर्जा सूचना केन्द्रको कालोसूचीमा समाविष्ट गर्नुपर्ने सम्बद्ध सबैलाई नेपाल राष्ट्र बैंकको निर्देशिका बमोजिम कर्जा सूचना केन्द्रको कालोसूचीमा समावेश गराउन सकिने व्यहोरा जानकारी गराउँदै कर्जाको सुरक्षणको रुपमा बैंक समक्ष धितो रहेको तपसिलमा उल्लिखित अचल जायजेथा जे जस्तो अवस्थामा छ सोही अवस्थामा बैंक तथा वित्तीय संस्था सम्बन्धी ऐन, २०७३ तथा अन्य प्रचलित कानूनले दिएको अधिकार प्रयोग गरी प्रस्तुत सूचनाको म्याद भित्र प्राप्त हुन आएका गोप्य शिलवन्दी बोलपत्रको माध्यमवाट लिलाम बिक्री गरिने र कुनै कारणवश तपसिलमा उल्लिखित जायजेथा लिलाम बिक्री नभएमा सो जायजेथा अन्य व्यवस्था गरी बेच बिखन गर्न सक्ने वा नियमानुसार बैंकले आफ्नो नाममा सकार गरी लिन सक्ने तथा उक्त जायजेथाबाट बैंकको सम्पूर्ण बक्यौता असूल उपर नभएमा प्रचलित कानून बमोजिम असुल उपर गरी लिइने व्यहोरा समेत जानकारी गराइन्छ

तपसिल

ऋणी तथा जमानतकर्ताको विवरण :	
१ ऋणी: हिरु मल्ल (ना.प्र.नं.२३४६/४०४), जारी मिति २०५०/११/०१, जि.प्र.का. रुकुम) स्थाई ठेगाना : रुकुम जिल्ला, घेत्मा गा.वि.स. वडा नं. ८ हालको ठेगाना : रुकुम पश्चिम जिल्ला, आठबिसकोट न.पा वडा नं. १३। बाबु : कृष्ण मल्ल। बाजे : हर्कु मल्ल।	**जमानतकर्ता : श्रीमती सरस्वती मल्ल** (ना.प्र.नं. ५६३०३५/३७१, जारी मिति २०६३/१०/२८, जि.प्र.का. रुकुम)। स्थाई ठेगाना : रुकुम जिल्ला, घेत्मा गा.वि.स. वडा नं. ८ हालको ठेगाना : रुकुम पश्चिम जिल्ला, आठबिसकोट न.पा वडा नं. १३। बाबु : सर्पु चन्द। पति : हिरु मल्ल। ससुरा : श्री कृष्ण मल्ल।
लिलाम बिक्री हुने सम्पत्तिको विवरण : **हिरु मल्ल**को नाममा मालपोत कार्यालय रुकुममा दर्ता श्रेष्ता कायम रहेको रुकुम जिल्ला घेत्मा गा.वि.स. वडा नं. ७, नक्सा सीट ५४२ स्थित कित्ता नं. ८८० क्षेत्रफल ०२३८५ (वर्ग मि.) को घर/जग्गा र सो घर/जग्गा समेत सम्पूर्ण लिगलगापात समेत १	
पुनश्च : १. बोलपत्र सम्बन्धी शर्त बन्देज सहितको बोलपत्र फारम बैंकको **प्रधान कार्यालय, बबरमहल, काठमाण्डौ स्थित कर्जा असुली विभाग र शाखा कार्यालय, आठबिसकोट, रुकुम (पश्चिम)बाट** समेत प्राप्त गर्न सकिनेछ। २. सम्पत्ति दाखेलखारेज नामसारी गर्दा नेपाल सरकारले तोके बमोजिम लाग्ने राजश्व लगायत सम्पूर्ण दैदस्तुर सकार कर्ता स्वयंले तिर्नुपर्नेछ। ३. लिलाम हुने सम्पत्ति निरीक्षण अवलोकन गर्नु परेमा वा धितो लिलाम सम्बन्धी अन्य थप जानकारी आवश्यक भएमा बैंकको **प्रधान कार्यालय, बबरमहल, काठमाण्डौ स्थित कर्जा असुली विभाग र शाखा कार्यालय आठबिसकोट, रुकुम (पश्चिम)मा** सम्पर्क राख्न सकिनेछ।	

PRABHU BANK

प्रभु बैंक लिमिटेड
प्रधान कार्यालयः बबरमहल, काठमाडौं, नेपाल
फोन नं. ०१-५७१९०००