FREEDOM FORUM

"A Nepali CSO (civil society organization) dedicated to democracy, human rights and governance"

पत्रकारका लागि डिजिटल सुरक्षा

सम्बन्धी उपयोगी जानकारी

फ्रिडम फोरम
थापाथली, काठमाडौं, नेपाल
पोष्ट बक्स: २४२९२
फोन: ४१०२०३०/४१०२०२२
इमेल: info@freedomforum.org.np
www.freedomforum.org.np
www.nepalpressfreedom.org
RTI Nepal App
Freedomchautary Podcast

असार, २०७९

भूमिका

फ्रिडम फोरमले गरेको सर्वेक्षणमा प्राप्त विवरण अनुसार प्रत्येक १० नेपाली पत्रकारमध्ये ७ जनाले डिजिटल स्पेसमा चुनौती (असुरक्षा) महशुस गरेको बताएका छन् । अझ खोज पत्रकारहरु र पत्रकार महिलाहरुले कतिपय अवस्थामा झन् बढी खतराको सामना गर्नुपर्ने पनि हुनसक्छ । डिजिटल स्पेसको बढ्दो प्रयोगसँगै परम्परागत अपराध पनि नयाँ स्पेसमा सरेका छन्, जुन खोज पत्रकारका लागि नयाँ चुनौतीको रुपमा प्रकट भएको छ । अर्कोतिर सूचना र सञ्चार प्रविधिका माध्यमहरुबाट राज्यका सुरक्षा निकाय र विभिन्न सेवा निकायहरुबाट समेत पनि कतिपय निगरानी (surveillance) का कारणले पत्रकारहरुको गोपनीयता जोखिममा परेर डिजिटल असुरक्षा तथा चुनौती थपिएको देखिन्छ ।

विश्वका विभिन्न देशमा पत्रकारहरुले थुप्रै डिजिटल जोखिम जस्तैः दूर्व्यवहार, सूचना तथा तथ्यांक चोरी, ह्याकिङ्, फिसिङ, मालवेयर, स्पाइवेयर भोगेका समाचारहरु आइरहेका छन् । फ्रिडम फोरमको नियमित अनुगमनले पनि नेपाली पत्रकारमाथि पछिल्लो समयमा डिजिटल माध्यमबाट हुने दूर्व्यवहार र धम्की जस्ता थ्रेट बढेको देखाएको छ । त्यसैगरी डिजिटल साक्षरताको कमीले सुरक्षाको लागि सामान्य उपायहरुको अवलम्बन गर्न नसक्दा नेपाली पत्रकारहरुले डिजिटल असुरक्षाको बढ्दो चुनौती सामना गर्नुपर्ने खतरा छ ।

फ्रिडम फोरमले पत्रकारहरुको डिजिटल सुरक्षामा आएका यिनै नयाँ चुनौतीलाई सामना गर्न सहयोग पुगोस् भनी यो स्रोत सामाग्री तयार गरेको हो । हाम्रो उद्देश्य यी स्रोत सामाग्रीको सही प्रयोग होस् र सुरक्षित डिजिटल स्पेसको निर्माण होस् भन्ने हो । यी सामाग्री अभिव्यक्ति स्वतन्त्रता तथा पत्रकारको सुरक्षामा काम गर्ने विश्वव्यापी सञ्जाल आइफेक्स (IFEX-International Freedom of Expression Exchange) का विभिन्न देशका सदस्य संस्थाहरुले तयार र वितरण गरेका स्रोत सामाग्रीहरुबाट लिई सो को नेपाली सन्दर्भमा उपयोगी हुनेगरी सम्पादनसहित यस पुस्तिकामा प्रस्तुत गरिएका हुन् ।

१. आफ्नो इमेल अकाउन्ट कसरी सुरक्षित गर्ने?

- आफ्नो व्यक्तिगत र व्यवसायिक जानकारी मिसिन नदिनुहोस् ।
- आफ्नो गोपनीयता सेटिंगहरु बेलाबेलामा समीक्षा गरी परिमार्जन गर्नुहोस् ।
- कुनै जानकारी सार्वजनिक रुपमा राख्नु अगाडि राम्रोसँग विचार गर्नुहोस ।
- आफ्नो पासवर्डहरुलाई सुरक्षित तरिकाले नोट गरेर राख्नुहोस् ।
- आफुसँग सम्बन्धित सार्वजनिक जानकारीको बेलाबेलामा समीक्षा गरी, राख्न आवश्यक नभएकालाई मेटाउनुहोस् ।
- सजिलै अनुमान गर्न सकिने पासवर्ड नराखी बलियो पासवर्डको प्रयोग गर्नुहोस् ।
- दुई-तह प्रमाणीकरण (Two step verification) गर्नुहोस् ।
- अनाधिकृत पहुँचबाट जोगिन अकाउन्ट प्रयोगपछि प्रत्येक पटक लग आउट गर्नुहोस् र Browsing History मेटाउनुहोस् ।
- अन्य व्यक्तिले आफ्नो Account प्रयोग गरेको थाह पाउन, Account Activities नियमित जाँच गर्ने गर्नुहोस् ।
- सार्वजनिक रुपमा राखिएका कम्प्युटरहरुमा आफ्नो Account सकेसम्म नखोल्नुहोस्, खोल्नै परेमा तुरुन्त लग आउट गरी Browsing History मेटाउनुहोस् ।

२. फिसिंग आक्रमण विरुद्ध कसरी सुरक्षित रहने ?

(फिसिंग भनेको जालसाजी गरी व्यक्तिको गोप्य जानकारी जस्तै पासवर्ड वा बैंक खाता सम्बन्धी सम्पूर्ण जनकारी पत्ता लगाउने तरिका हो ।)

- अनधिकृत रुपमा पटक-पटक आएका जोखिमयुक्त म्यासेजबाट सावधान हुनुहोस् । तथा लिङ्क थिच्न वा Attachment download गर्नु पूर्व सोच विचार गर्नुहोस् ।
- जोखिमयुक्त म्यासेज पठाउने व्यक्तिको प्राविधिक क्षमताको अनुसन्धान गर्नुहोस् ।
- पठाउनेको Account विवरण र सन्देश सामाग्री वैध छ वा छैन भन्ने विचार गर्नुहोस् ।
- शंकास्पद लागेका म्यासेजबारे पठाउने व्यक्ति वा संस्थालाई सम्पर्कगरी हो-होइन निश्चित गर्नुहोस् ।
- कुनै लिङ्कमा क्लिक गर्नु अघि सावधानीसाथ त्यसको विश्वासनियता बारे विचार गर्नुहोस् ।
- चुनाव र राजनीतिक अस्थिरताको अवस्था तथा भ्रष्ट्राचार र अनियमितता सम्बन्धी खोजी रिपोर्टिङ गर्दा फिसिंगको खतराबाट विशेष रुपमा सतर्क रहनुहोस् ।

३. यन्त्र-उपकरण (कम्प्युटर, ल्यापटप, मोबाइल आदि) कसरी सुरक्षित गर्ने ?

- पासवर्ड, कोड वा PIN मार्फत् आफ्नो उपकरणहरू लक गर्नुहोस् । लामो PIN वा पासवर्डहरु प्रयोग गर्नुहोस् ।
- पुरानो सफ्टवेयरको कमजोरीबाट माल्वेयर (malware) छिटो फैलिन सक्ने भएकोले समयमा आफ्नो अपरेटिंग सिस्टम, एप र ब्राउजर अपडेट गर्ने गर्नुहोस् ।
- आफ्नो डिभाइसमा स्टोर भएको जानकारीहरुको बेलाबेलामा समीक्षा गर्नुहोस् ।

साथै, आफूलाई जोखिममा पार्नसक्ने वा संवेदनशील सूचना आवश्यकता अनुसार डिलिट गर्ने वा ब्याकअपमा राख्ने गर्नुहोस् ।

- च्याटहरु जस्ता संवेदनशील जानकारी नियमित रुपमा मेटाउनुहोस् ।
- चोरी वा दुरुपयोग हुनसक्ने ठाउँहरुमा आफ्नो डिभाइस नछोड्नुहोस् ।
- सार्वजनिक USB पोर्टहरुमा उपकरण प्रयोग नगर्नुहोस् । कार्यक्रमहरुमा निशुल्क उपलब्ध गरिएको USB फ्ल्यास ड्राइभहरु पनि प्रयोग नगर्नुहोस ।
- उपकरणहरुको मर्मत गर्दा विश्वासिलो व्यक्ति वा ठाउँमा मात्र गर्नुहोस् ।

४. यन्त्र- उपकरण Encrypt कसरी गर्ने ?

- नयाँ स्मार्टफोनहरुमा Encryption को सुबिधा हुन्छ यसलाई सेटिङमा गई Activate गर्नुहोस् ।
- Windows मा Bitlocker, Mac मा Firevault, वा Hard drive र External device को लागि नि:शुल्क पाइने Veracrypt सफ्टवेयरको प्रयोग गरी Encrypt गर्नुहोस् ।
- Encryption का लागि लामो र बलियो पासवर्ड प्रयोग गर्नुहोस् ।
- तपाई यात्रा गरिरहनु भएको देशमा Encryption सम्बन्धी कानुन के छ भनी पहिले नै जानकारी लिनुहोस् ।

५. Encrypted सामाग्री सञ्चार कसरी गर्ने ?

- एपको स्वामित्व कसले राख्छ, उनीहरूले प्रयोगकर्ताको कुन डाटा राख्छन् र त्यो डाटा सरकारलाई पेश गर्ने गरिएको छ कि छैन भनेर अध्ययन गर्नुहोस् ।
- प्रयोगकर्ता डाटा सेयर गर्न आउने अनुरोधहरूको प्रतिक्रिया दिनु अगाडि तिनीहरूको नीति के हो भनेर जाँच गर्नुहोस् ।
- प्रविधि कम्पनीहरूले हटाउने वा साझोदारी गर्ने बारेका सरकारी अनुरोधको कारबाही बारे प्रत्येक वर्ष पारदर्शिता प्रतिवेदन तयार गर्नुपर्छ । सो प्रतिवेदन बारे पनि जानकारी राख्नुहोस् ।

- अर्को व्यक्तिबाट एप खोल्न सक्ने जोखिम भएमा सुरक्षित हुन सम्भव भएसम्म PIN वा पासकोडको साथ एप लक गर्नुहोस् ।
- यदि कुनै पनि एपमा Registration Lock को व्यवस्था छ भने सेटअप गर्नुहोस् ।
- Signal र WhatsApp लगायतका केही एपहरूले तपाईं को सँग च्याट गर्दै हुनुहुन्छ भनी पुष्टि गर्नको लागि थप सुरक्षा तह प्रदान गर्दछ र कसैलाई अर्को डिभाइसबाट तपाईंको नक्कल गरी सम्पर्क गर्नबाट रोक्छ ।
- तपाईंलाई पठाइएका तस्विरहरू वा कुनै डकुमेन्ट तपाईंको डिभाइसमा कहाँ भण्डारण हुन्छ भनेर बुझ्नुहोस् ।
- जब तपाईं आफ्नो डाटा ब्याकअप गर्नुहुन्छ, तपाईंले डाउनलोड गर्नु हुने कुनै पनि कुरा, जस्तै फोटोहरू, तपाईंको डिभाइसमा सुरक्षित हुन्छन् र अन्य डिभाइस र एपमा पनि तिनको Copy सुरक्षित हुन सक्छ । यी कुरामा ध्यान दिनुहोस् ।
- केही सेवाहरू, जस्तै WhatsApp, टेलिफोन नम्बरसँग लिङ्क गरिएको क्लाउड अकाउन्टमा तपाईंको सन्देश सामग्री ब्याकअप हुन्छ । iOS प्रयोगकर्ताहरूको Signal मा कुनै पनि कल History iCloud सँग sync हुन्छ । एपको सेटिङमा गएर यसलाई बन्द गर्न पनि सकिन्छ ।
- तपाईंको फोनमा भण्डार गरिएका सम्पर्क र सन्देशहरु क्लाउड अकाउन्टहरूसँग sync हुन्छन्, त्यसैले तपाईंले सम्पर्क गरेका नम्बरहरू एक ठाउँबाट मेटाए पनि अन्त कतै सुरक्षित रहन्छ, तसर्थ सबै तिरबाट ती कुराहरु मेटाउनुहोस् ।
- डिभाइस वा Account मा सकेसम्म थोरै भण्डार गर्नका लागि सन्देशहरू नियमित रूपमा ब्याक अप गर्नुहोस् र मेटाउनुहोस् ।
- डकुमेन्ट, फोटो, भिडियो, अडियो म्यासेजहरु कुन राख्ने कुन नराख्ने भन्ने निर्णय गर्नुहोस् । राख्नुपर्ने डकुमेन्ट, फोटो, भिडियो, अडियो म्यासेजहरु Encrypted हुने डिभाइसमा राख्नुहोस् ।
- Signal, WhatsApp, Messenger मा निश्चित समय पछि सन्देशहरू स्वचालित रूपमा मेटाउन मिल्ने option रहन्छ ।
- Signal, WhatsApp, Viber ले end–to–end Encrypted भिडियो कलको सुविधा दिन्छन् ।

६. Encrypted इमेलको प्रयोग

- इमेल सेवाको लागि विश्वसनीय Encryption सफ्टवेयर छान्नुहोस् ।
- Encrypted इमेल सफ्टवेयरको लागि Strong र Unique पासवर्ड प्रयोग गर्नुहोस् । यदि पासवर्ड बिर्सनुभयो भने Encrypted इमेलहरूमा पहुँच गुम्नेछ, त्यसैले सचेत रहनुहोस् ।
- Sender र Receiver को इमेल ठेगाना र इमेलको शीर्षक भने Encrypted हुदैँनन् ।

७. सुरक्षित इन्टरनेट प्रयोग कसरी गर्ने ?

- प्रत्येक वेभसाइट को सुरुमा https:// र प्याडलक आइकन छ/छैन हेर्नुहोस् । यसले तपाईं र साइट बीचको ट्राफिक Encrypted गरिएको छ भनी संकेत गर्दछ । यस्ता वेभसाइट चलाउनु सुरक्षित हुन्छ ।
- तपाईं कुनै असुरक्षित साइटहरू (http://) खोल्दै हुनुहुन्छ भने आफ्नो ब्राउजरमा HTTPS Everywhere भन्ने Extension को प्रयोग गर्नुहोस् । यसबाट तपाईको ब्राउजर सुरक्षित हुनेछ । जस्तै:

eff.org ⟶ tools ⟶ Https ⟶ Everywhere Install on chrome

- Pop-up विज्ञापनहरूमा लुकेको मालवेयरबाट आफ्नो Device जोगाउन विज्ञापन-ब्लकर install गर्नुहोस् ।
- असुरक्षित वेभसाइट र विज्ञापनलाई तपाईंले प्रयोग गर्नुभएको साइट ट्रयाक गर्नबाट रोक्न Privacy Badger Picture install गर्नुहोस् ।

- प्रयोगमा नभएको बेला Bluetooth र अन्य File Sharing App तथा डिभाइस बन्द गर्नुहोस् ।

- इन्टरनेट ट्राफिकलाई इन्टरनेट सेवा प्रदायकद्वारा अनधिकृत रुपमा लगइन हुनबाट सुरक्षित गर्न VPN प्रयोग गर्नुहोस् ।
- सार्वजनिक स्थलमा राखिएका कम्प्युटरहरू प्रयोग नगर्नुहोस्, विशेष गरी इन्टरनेट क्याफे वा सञ्चार गृहहरुमा साझा कम्प्युटरहरू प्रयोग गर्नु परेमा सबै डिभाइसबाट लग आउट गर्नुहोस् र आफ्नो ब्राउजिङ History पूर्णरुपमा मेटाउनुहोस् ।
- गोप्य रूपमा इन्टरनेट प्रयोग गर्नु परेमा निःशुल्क ToR Browser Bundle install गर्नुहोस् । ToR मार्फत तपाइँको सबै इन्टरनेट ट्राफिकलाई रुट गर्ने निःशुल्क अपरेटिङ सिस्टम हो । ToR विशेष गरी अनुशन्धानमूलक विषयहरूको रिपोर्टिङ गर्ने पत्रकारहरुका लागि सिफारिस गरिएको छ । ToR प्रयोग गर्ने सम्बन्धमा तपाईं रहनु भएको देशको कानुनको बारेमा पनि जानकारी लिनुहोस ।

८. Virtual Private Network को प्रयोग कसरी गर्ने ?

VPN एक भर्चुअल निजी नेटवर्क हो । यसले सार्वजनिक इन्टरनेट जडानबाट एक निजी नेटवर्क सिर्जना गरेर तपाईंलाई अनलाइनमा गोपनीयता र अनामता (anonymity) को सुविधा दिन्छ । VPN ले तपाईको इन्टरनेट प्रोटोकल (IP) ठेगाना लुकाउँछ त्यसैले तपाईका अनलाइन कार्यहरू पत्ता लगाउन सकिँदैन ।

सबैभन्दा महत्वपूर्ण, VPN सेवाले सुरक्षित Wi–Fi हटस्पट का साथै गोपनीयता कायम राख्न सुरक्षित र इन्क्रिप्टेड जडानहरू उपलध गराउँछ ।

- कुनै VPN सेवा लिनु अघि सो को गुणस्तर र सुरक्षाबारे राम्रोसँग बुझ्नुहोस् ।
- VPN को स्वामित्व, तीनले तपाईंको ब्राउजिङ History राख्छन् की राख्दैनन् र सो कम्पनीले सरकारसँग डाटा साझेदारी गर्दछ कि गर्दैन भन्ने विषयमा अध्ययन गरी जानकार हुनुहोस् ।
- त्यस्तो VPN छनौट गर्नुहोस् जसले तपाईंको डाटाको रेकर्ड राख्दैन ।
- तपाईले काम गरिरहनु भएको देशमा अवस्थित नभएको VPN सेवा प्रयोग गर्नुहोस् र यसको सर्भरहरू पनि देश बाहिर अवस्थित छन् कि छैनन् बुझ्नुहोस् ।
- VPN प्रयोग गर्दा, नजिकैको देशबाट Navigate गर्न चयन गर्नुहोस् ।

- केही देशहरूमा यो VPN प्रयोग गैह्न कानुनी मानिन्छ । तपाई जान लागेको देशको यस सम्बन्धी कानुनबारे जानकारी लिनुहोस ।
- सरकारले स्वीकृति दिएका VPN ले तपाईंको ब्राउजिङ History र location रेकर्ड गर्ने र यी सूचना, अधिकारीहरूलाई पास गर्ने खतरा धेरै हुन्छ ।
- यो सेवामा इन्टरनेट सेवा प्रदायकले तपाई अनलाइनमा के हेर्दै हुनुहुन्छ भनेर हेर्न त सक्दैन तर तपाई इन्टरनेटमा जोडिनु भएको थाहा हुन्छ ।
- फोनमा VPN प्रयोग गर्दा तपाई के हेर्दै हुनुहुन्छ भनेर लुकाउँछ, तर तपाईंको मोबाइल फोन कम्पनीले भने तपाइँको स्थानको रेकर्ड राखिरहेको हुन्छ ।

९. Password Manager भनेको के हो ?

- **Password Manager** पासवर्ड व्यवथापन गर्ने सबैभन्दा सुरक्षित तरिका हो । यो एउटा एप हो जुन तपाई आफ्नो डिभाइसमा डाउनलोड गर्न सक्नुहुन्छ । यसले बलियो पासवर्ड बनाउन र भण्डारण गर्न सहयोग गर्छ। तर, तपाईले यस प्रबन्धकको लागि पनि unique र strong पासवर्ड बनाउनु पर्छ।

- केहि पासवर्ड प्रबन्धक App हरु:
  - Last Pass
  - 1 Password
  - Common Key

१०. बलियो पासवर्ड कसरी बनाउने ?

- पासवर्ड कम्तिमा आठ अक्षर वा अङ्क वा चिन्ह मिश्रित बनाउनुहोस् उदाहरणको लागि : #ClB46@FF ।
- शब्दकोशमा रहेका सरल र सहजै अनुमान गर्न सक्ने शब्दहरू प्रयोग नगर्नुहोस् ।
- Upper case र lower case अक्षरहरू, अङ्कहरू र चिन्हहरूको प्रयोग गरी आफ्नो पासवर्ड सुरक्षित बनाउनुहोस् ।

- बेला-बेलामा पासवर्डहरू परिवर्तन गर्नुहोस् । प्रत्येक तीन महिनामा Password Manager को प्रयोग गर्नुहोस्, जसले तपाईंलाई एउटा Master पासवर्ड मार्फत्

अन्य सबै पासवर्डहरूलाई सुरक्षित रूपमा भण्डार गर्नुका साथै सम्झिन सहयोग गर्दछ ।

- दुई-तह प्रमाणीकरण (Two-step verification भन्नाले तपाईंको मोबाइल फोन र इमेल दुवै बाट verify गर्ने) को प्रयोग गर्नुहोस्

- The Dice Method र The Person, Action, Object method प्रयोग गरेर पनि पासवर्ड बलियो बनाउन सकिन्छ ।
  - **The Dice Method**: आफ्नो इच्छा अनुसार दुईवटा देखि आठ वटा Dice हरु रोल गर्नुहोस् र प्राप्तसंख्या अनुसारको शब्द सूचीबाट चयन गर्नुहोस । तपाईंले जति धेरै शब्दहरू चयन गर्नुहुन्छ, पासवर्ड त्यति बलियो हुन्छ । Diceware (https://diceware.dmuth.org/) ले यो विधि कसरी प्रयोग गर्ने भनेर सहयोग गर्छ ।
  - **The Person, Action, Object Method :** यो विधि अनुसार पहिले एउटा रोचक ठाउँ चयन गर्नुपर्छ, दोस्रोमा परिचित वा प्रसिद्ध व्यक्तिको चयन गर्नुपर्छ र त्यसपछि अन्त्यमा कुनै वस्तुको नाम र त्यससँग सम्बन्धित सामान्य कार्यको कल्पना गरी पासवर्डको सिर्जना गर्न सकिन्छ ।

सुरक्षा विधि अपनाउन प्रयोग हुने सफ्टवेयरहरु के के हुन् ?

१. सूचनाको सुरक्षित भण्डारण गर्न

- Bitlocker - यसले Windows अपरेटिङ सिस्टम भएका कम्प्युटरहरूको encryption गर्दछ । यो Windows Vista, 8.0, 8.1 Pro, 10 र Enterprise editions, र Windows Servers 2012 R2 मा पाइने सफ्टवेयर हो ।
- File Vault - यसले अपरेटिङ सिस्टम (OS) सँग कम्प्युटरहरूको encryption गर्छ । यसको लागि OS Lyon वा अझ आधुनिक OS अपरेटिङ सिस्टम चाहिन्छ ।
- Veracrypt - Bitlocker or File Vault लाई support नगर्ने Windows वा OS अपरेटिङ सिस्टमहरू भएका कम्प्युटरको encryption गर्न यो सहयोगी छ ।

२. सुरक्षित एन्टिभाइरसको प्रयोग

- Avira: यो मालवेयर छेक्न र भाइरस पत्ता लगाउन व्यक्तिगत प्रयोगको लागि एक निःशुल्क सफ्टवेयर हो ।
- Clam AV/Immunet: यो ट्रोजन, भाइरस, मालवेयर र अन्य खतराहरू पत्ता लगाउनका लागि पाइने निःशुल्क एन्टिभाइरस हो ।
- Avast: यो कम्प्युटर र मोबाइल फोनहरू (एन्ड्रोइड र iOS अपरेटिङ सिस्टम दुवैको लागि) सुरक्षित गर्न प्रयोग हुने निःशुल्क एन्टिभाइरस हो ।

- Symantec Endpoint Protection: यो स्तरीय र खुफिया सुरक्षा प्रदान गर्ने व्यवसायिक antivirus र firewall सेवा हो ।
- AVG: यो निःशुल्क पाइने एन्टिभाइरस र एन्टिस्पाइवेयर सुरक्षा सफ्टवेयर हो । पत्रकारहरुले पैसा तिरेर यसको विशेष सेवा (जस्तै इन्टरनेट सुरक्षा) लिन सक्छन् ।
- Spybot: यो पनि निःशुल्क antimalware र antispyware उपकरण हो ।

४. इन्टरनेट सुरक्षा कसरी हुन्छ?

- TOR: यो ट्राफिक विश्लेषण विरुद्ध प्रयोगकर्ताहरूको रक्षा गर्ने एक निःशुल्क सफ्टवेयर हो । यसले प्रयोगकर्ताको पहिचान लुकाउँछ र इन्टरनेट फिल्टरहरूलाई बाइपास गर्छ ।
- Anonymox: यो Firefox र Chrome वेब ब्राउजरहरूको लागि प्रयोगकर्ताको पहिचान लुकाउन, आईपी गोप्य राख्न र इन्टरनेट नेभिगेसनको सुरक्षा गर्नको लागि निःशुल्क उपलब्ध plugin हो ।
- Riseup/ VPN: यो सेन्सरशीप कर्पोरेट निगरानी तथा नियमनबाट जोगाउनका लागि इन्क्रिप्टेड Riseup.net सर्भरहरू मार्फत इन्टरनेटमा प्रयोगकर्ता नेभिगेसन सुरक्षित गर्न सकिने निःशुल्क सफ्टवेयर हो ।

५. Anonymous search engines (गोप्य खोज इन्जिनहरू के के हुन् ?)

- DuckDuckGo: यो Encrypted वेभ खोज इन्जिन हो, जसले इन्टरनेटमा तपाईले खोजेका सामाग्रीहरुको गोप्यता कायम राख्छ । यसले फायरफक्स ब्राउजरमा add-on को रूपमा काम गर्छ ।
- StartPage: यो पनि तपाईले इन्टरनेटमा खोज्नुभएका सामाग्रीहरुको गोपनीयताको रक्षाको लागि बनाइएको Encrypted खोज इन्जिन हो ।

६.सञ्चार सुरक्षा एपहरु के के हुन् ?

(क) इमेल

- Gmail सुरक्षा जाँच
- Gmail Two-step verification
- Google advanced protection
- Thunderbird ± GnuPG ± Enigmail
- Mailvelope
- Protonmail

(ख) सुरक्षित सन्देश

- Pidgin वा Adium ± OTR

(ग) एन्क्रिप्टेड भिडियो सम्मेलन

- MeetJitsi

(घ) मोबाइल उपकरण सुरक्षा

- Lookout
- Avast -for Android
- Avira

(ङ) सुरक्षित इन्टरनेट नेभिगेसन

- Psiphon for Android
- Private Internet Access

(च) गोप्य नेभिगेसन (Anonymous navigation)

- Orfox
- iOS को लागि Onion Browser

(छ) सुरक्षित मोबाइल च्याट

- Chat Secure च्याट सुरक्षित (एन्ड्रोइड र iOS का दुवैका लागि)
- Secure SMS
- Signal

(ज) इन्क्रिप्टेड फोन कल

- Signal iPhone र Android का लागि बलियो encryption
- Whatsapp: encryption संचार मार्फत तुरुन्त सन्देश र कल गर्न

६.स्रोतहरूको सुरक्षा कसरी गर्ने ?

- यदि तपाई इन्टरनेट सुरक्षाको विषयमा कम जानकार स्रोतहरूसँग सञ्चार गर्दै हुनुहुन्छ भने, उनीहरुसँग इमेल मार्फत सञ्चार गर्न यी तरिकाहरु अपनाउनुहोस् :

१. https://protonmail.com मा आफ्नो लागि Proton mail account बनाउनुहोस् ।

२. आफ्नो स्रोतलाई सुरक्षित पासवर्डहरू सिजना गर्न भन्नुहोस् ।

३. यदि तपाईंको स्रोतले सार्वजनिक स्थानमा भएको कम्प्युटरबाट Protonmail प्रयोग गर्दैछन् भने उनीहरुलाई निजी/incognito मोड प्रयोग गर्न लगाउनुहोस् र attachment व्यक्तिगत USB मा राख्न सुझाउनुहोस् ।

- यदि तपाइँ इन्टरनेट सुरक्षाको विषयमा राम्रो जानकारी भएको स्रोतहरूसँग कुराकानी गर्दैहुनुहुन्छ भने, उनीहरूलाई PGP (Pretty Good Privacy) सक्रिय गर्न लगाउनुहोस् । यसले तपाईलाई सार्वजनिक पासवर्ड सेटअप गर्न र चाहिएका डकुमेन्टलाई विद्युतीय हस्ताक्षर गरी प्रमाणीकरण गर्न सहयोग गर्दछ ।
- आफ्नो मोबाइल फोन र कम्प्युटर/ल्यापटपमा कन्ट्याक्ट लिस्टको पहुँच गर्न सुरक्षित पासवर्ड बनाउनुहोस् ।
- पाइरेटेड वा शंकास्पद सफ्टवेयर डाउनलोड नगर्नुहोस्, यसले तपाईंको डाटा जोखिममा पर्छ ।

७. मोबाइल फोनको सुरक्षा कसरी गर्ने ?

- आफ्नो मोबाइल फोन पासवर्डले सुरक्षित गर्नुहोस् । यसको लागि पनि अंक, अक्षर र चिन्हहरुको संयोजन गरी बनेको पासवर्ड सबैभन्दा सुरक्षित विकल्प हो । मोबाइल फोन प्रयोग गर्न मात्र होइन त्यसमा रहेका एप (इमेल, सामाजिक सञ्जाल आदि) मा प्रवेश गर्न पनि पासवर्डहरू राख्नुहोस् ।
- थप सुरक्षाको लागि आफ्नो SIM कार्डलाई SIM पिन कोडद्वारा सुरक्षित गर्नुहोस्, फोनको सेटिङ्गमा यो सुविधा उपलब्ध हुन्छ ।
- अत्यधिक संवेदनशील जानकारी च्याटमा कहिल्यै share नगर्नुहोस् । जस्तै- तपाईको बैंक जानकारी वा तपाईको पासवर्डहरु, आदि ।
- End-to-End इन्क्रिप्सन गर्ने एपहरू जस्तै Signal वा Wire मार्फत मात्र अरूसँग कुराकानी गर्नुहोस् ।

फ्रिडम फोरम अनुसन्धान एवं वकालतकर्ता प्राज्ञिक समुदायको साझा पहल हो । लोकतन्त्र, मानवअधिकार, प्रेस स्वतन्त्रता र राष्ट्रको समविकासमा समर्पित रहने उद्देश्यले २०६२ सालमा यसको स्थापना भएको हो । मानव स्वतन्त्रताको उच्चतम मूल्यप्रति प्रतिवद्ध पत्रकार, कानुन व्यवसायी, मानव अधिकारकर्मी, प्राध्यापक-शिक्षक, समाजशास्त्री तथा विकास कार्यकर्ताहरुको साझा मञ्चका रूपमा यो फोरम स्थापना गरिएको हो। प्रेस तथा अभिव्यक्ति स्वतन्त्रता, सूचनाको हक, वजेट पारदर्शिता, निर्वाचन तथा लोकतान्त्रिक शासन प्रणाली, सार्वजनिक वित्त व्यावस्थापन, डिजिटल स्वतन्त्रता र सामाजिक जवाफदेहिता प्रवर्द्धनका गतिविधिमार्फत आम जनतालाई लोकतन्त्रको प्रतिफल प्राप्त गर्ने अवस्थामा पुऱ्याउन यो संस्था प्रयासरत छ । समुन्नत लोकतान्त्रिक समाज यसको लक्ष्य हो । मुलुकका विभिन्न क्षेत्रमा छरिएर रहेका स्वतन्त्रताका पुजारीहरु यसका सदस्य वन्न सक्छन् । नागरिक समाज, आमसञ्चार, पेसागत क्षेत्र र तल्लो तहका सामुदायिक संगठनसँग सहकार्य गरेर अगाडि वढ्ने हाम्रो नीति रहेको छ । सम्पुर्ण स्वतन्त्रता मानव सभ्यताको अनन्त चाहना हो । स्वतन्त्रताभन्दा मूल्यवान अरू केही छैन भन्ने फ्रिडम फोरम ठान्छ ।

फ्रिडम फोरम
थापाथली, काठमाडौं, नेपाल
पोष्ट वक्स: २४२९२
फोन: ४१०२०३०/४१०२०२२
इमेल: info@freedomforum.org.np
www.freedomforum.org.np
www.nepalpressfreedom.org