डिजिटल प्रविधिहरू सुरक्षित, बुद्धिमत्तापूर्वक र जिम्मेवारीपूर्वक प्रयोग गर्ने तरिका:

नागरिक समाज संस्थाहरूका लागि छोटो मार्गदर्शन

टिम अनविन

ICT4D कलेक्टिभको तर्फबाट

https://ict4d.org.uk

संस्करण ४

अगस्ट २०२४

CC BY SA

ICT4D Collective

यो "हुन्छ कि हुँदैन" भन्ने प्रश्न होइन, तर "कहिले" तपाईँको संस्थाले कुनै न कुनै प्रकारको साइबर आक्रमण भोग्नेछ भन्ने कुरा हो।

यो तपाईँको आफ्नै डिजिटल वातावरणभित्र प्रत्यक्ष हुन सक्दछ, वा तपाईँसँग काम गर्ने सङ्गठनमा भएको आक्रमणको माध्यमबाट पनि प्रभावित हुन सक्नुहुन्छ। त्यसैले आफ्ना कर्मचारी र तपाईँसँग काम गर्ने सबै व्यक्तिहरूलाई सुरक्षित राख्नका लागि आवश्यक सबै सावधानी अपनाउनु अत्यन्त महत्वपूर्ण छ। डिजिटल प्रविधिहरूले संस्थाहरूलाई धेरै लाभहरू प्रदान गर्न सक्छन् तर ती लाभहरू हासिल गर्नका लागि सम्भावित हानिहरूलाई न्यूनीकरण गर्नु अनिवार्य छ।

के यो सुरक्षित छ?

के यो विवेकपूर्ण छ?

के यसले सुरक्षा सुनिश्चित गरेको छ?

यो संक्षिप्त मार्गदर्शन मुख्यतः स्रोत–साधन सीमित भएका साना नागरिक समाज संस्थाहरूलाई डिजिटल प्रविधि सुरक्षित, विवेकपूर्ण तथा गोप्य रूपमा कसरी प्रयोग गर्ने भन्ने विषयमा आधारभूत सल्लाह प्रदान गर्न तयार गरिएको हो। यो मार्गदर्शन सबै–समावेशी वा अत्यधिक प्राविधिक हुनुको लागि नभइ सबै नागरिक समाज संस्थाहरूले आफ्नो प्राविधिक वा आर्थिक क्षमताबाट स्वतन्त्र रूपमा अपनाउनुपर्ने आधारभूत अभ्यासहरूमा केन्द्रित छ। मूलभूत साइबर सुरक्षा अत्यन्त आवश्यक छ र प्रविधि विकसित हुँदै जाँदा जोखिमहरू अझ बढ्दै जानेछन्। यी प्रमुख अभ्यासहरू अपनाउँदा तपाईँ आक्रमणबाट पूर्ण रूपमा सुरक्षित हुन सम्भव नहुन सक्छ तर यसले यस्ता आक्रमणहरूको सम्भावना र प्रभावलाई कम गर्नेछ र सम्भव भएसम्म छिटो पुनः अनलाइन हुन मद्दत गर्नेछ।

ICT4D Collective

तल उल्लेखित अवस्थाहरूमा तपाईँले कसरी प्रतिक्रिया जनाउनुहुन्छ वा तिनलाई कसरी रोक्न सक्नुहुन्छ?

तपाईँ घरेलु हिंसाबाट पीडित महिलाहरूलाई आश्रय प्रदान गर्ने एक नागरिक समाज संस्थाका संस्थापक हुनुहुन्छ। संस्थाको वेबसाइटमा आश्रयस्थलमा बसोबास गरिरहेका केही महिलाहरूका तस्बिरहरू राखिएका थिए र ती तस्बिरहरू सामाजिक सञ्जालमा पनि साझा भएका थिए। एक दिन ती महिलामध्ये एकजनामाथि पहिले हिंसा गरिसकेको पुरुष पनि सहभागी युवाहरूको समूहले आश्रयस्थलमा आक्रमण गर्‍यो। उक्त आक्रमणका कारण दुई महिलाको मृत्यु भयो ।

तपाईँ सडकमा बस्ने र बालश्रम जोखिममा रहेका बालबालिकालाई सहयोग गर्ने ठूलो सङ्गठन चलाउनुहुन्छ र कम्प्युटरमा तपाईँका सबै कर्मचारी सहयोगीहरू र उनीहरूको परिवारका सम्पर्क विवरणहरू राख्नुहुन्छ। एक दिन कार्यालय पुगेर सङ्गठनको मुख्य कम्प्युटर खोल्दा तपाईँले डेटा पहुँच गर्न सक्नुभएन र स्क्रिनमा ठूलो चित्र र सन्देश देखियो, जसमा भनिएको छ कि यदि ठूलो रकम तिर्नुभएन भने तपाईँको डेटा वेबमा सार्वजनिक गरिनेछ। त्यो रकम तिर्दा सङ्गठन आर्थिक रूपमा सङ्कटमा पर्न सक्छ र तपाईंको प्रतिष्ठा पनि जोखिममा पर्न सक्छ।

तलको मार्गदर्शन नोटहरू सरल र स्पष्ट राखिएका छन् र प्राविधिक भाषा कम प्रयोग गरिएको छ। **रातो** रङगमा देखाइएका सिफारिसहरू अनिवार्य छन् भने **निलो** रङगमा देखाइएका सिफारिसहरू धेरै महत्त्वपूर्ण मानिन्छन्।

तपाईँका लागि सबैभन्दा महत्वपूर्ण के हो ? त्यसलाई सुरक्षित राख्ने योजना।

माथि दिइएका उदाहरणहरूले देखाउँछन् जस्तै तपाईँले आफ्नो डिजिटल प्रणालीभित्र सबैभन्दा बढी सुरक्षित राख्नुपर्ने डेटा वा जानकारी के हो भनी सोचेर सुरु गर्नुपर्छ र त्यसलाई सुरक्षित राख्नको लागि योजना बनाउनुपर्छ। संवेदनशील विषयहरूमा काम गर्ने र जोखिममा रहेका व्यक्तिहरूसँग संलग्न संस्थाहरूका लागि ती व्यक्तिहरूको पहिचान सधैँ सुरक्षित राख्न र अरूको पहुँचबाट पूर्ण रूपमा जोगाउन आवश्यक हुन्छ। केहीका लागि फिल्डमा रहेका कर्मचारीहरूसँग सधैँ सम्पर्कमा रहन सक्ने व्यवस्था हुनु महत्त्वपूर्ण

ICT4D Collective

हुनसक्छ भने अरूका लागि ऐतिहासिक अभिलेखहरू भविष्यका लागि सुरक्षित रूपमा संरक्षण गरिएको सुनिश्चित गर्नु प्राथमिकता हुन सक्छ। तपाईँले कुन–कुन सूचना सङ्कलन गर्नुहुन्छ, किन गर्नुहुन्छ, र ती सबै सूचना अनलाइन राख्नु साँच्चिकै आवश्यक छ कि छैन भन्ने कुरा गम्भीर रूपमा सोच्नुपर्छ।

यदि सुरुवातमै तपाईँले आफ्ना शीर्ष पाँच प्राथमिकताहरू पहिचान गरेर तिनको सुरक्षा सुनिश्चित गर्ने प्रयास मात्र गर्नुभयो भने पनि तपाईँले एक महत्वपूर्ण कदम अघि बढाइसक्नु हुनेछ। तर कहिल्यै पनि डिजिटल प्रणाली प्रयोग गर्न नसक्ने अवस्था आएमा पनि सेवा प्रवाह र काम निरन्तर गर्न सकियोस् भनेर गैर–डिजिटल वैकल्पिक योजना (ब्याक–अप योजना) तयार राख्न नबिर्सनुहोस्।

यससँगै आफ्ना सबै कर्मचारी र सहकार्य गर्ने व्यक्तिहरूमा साइबर सुरक्षा संस्कृतिको विकास गर्नुहोस्। यसका लागि निर्णय प्रक्रियामा उनीहरूलाई सहभागी गराउनु महत्त्वपूर्ण हुन्छ ताकि उनीहरूले आफ्ना विचार दिन सकून् र तयार भएका निर्देशिका तथा अभ्यासहरूलाई आफ्नै रूपमा अपनाउन सकून्। तपाईँको योजनाले व्यक्तिगत रूपमा दोषारोपण गर्ने वा दण्ड दिने (जस्तै, सुरक्षा उल्लङ्घनका लागि कसैलाई दोष दिने) भन्दा पनि सामूहिक सहयोगमा केन्द्रित हुनुपर्छ, जसले सबैलाई राम्रो साइबर स्वच्छता अभ्यास अपनाउन सहयोग गर्छ।

यस उद्देश्यका लागि कार्यालय तथा सार्वजनिक स्थानहरूमा उपयुक्त र सान्दर्भिक साइबर सुरक्षा सम्बन्धी पोस्टर र नारा स्पष्ट रूपमा देखिने गरी राख्नु अत्यन्त उपयोगी हुन सक्छ (उदाहरण र थप स्रोतहरूका लागि परिशिष्ट हेर्नुहोस्)। यसले तपाईँको टिमभित्र आवश्यक साइबर सुरक्षा संस्कृतिको विकास गर्न सहयोग पुऱ्याउँछ र कार्यालयमा आउने आगन्तुकहरूमा पनि यी विषयमा चेतना बढाउन मद्दत गर्छ।

तपाईँले सामना गर्न सक्ने आक्रमणका प्रकारहरूबारे जानकार रहनुहोस्।

साइबर आक्रमण र ठगिका विभिन्न प्रकारहरू छन् तर नागरिक समाजका संस्थाहरूलाई प्रायः असर गर्ने सम्भावित आक्रमणहरू (वर्णानुक्रम अनुसार) यसप्रकार छन्:

- डीपफेक (Deep fakes): एआई प्रयोग गरी सिर्जना गरिएका तस्बिर, अडियो वा भिडिओमार्फत प्रतिष्ठामा क्षति पुर्याउने वा जनमत प्रभावित गर्ने प्रयास।

- पहिचान चोरी (Identity theft): आक्रमणकारीले तपाईँको पहिचान वा प्रमाणहरूमा पहुँच प्राप्त गरी तपाईँकै रूपमा प्रस्तुत हुनु। यो पहिचान गर्न कठिन हुन्छ किनकि आक्रमणकारीले तपाईँको सामान्य व्यवहार र पासवर्डको नक्कल गर्छ।

- मालवेयर (Malware): कम्प्युटर, नेटवर्क वा सर्भरमा क्षति पुऱ्याउने उद्देश्यले बनाइएका कुनै पनि हानिकारक प्रोग्राम वा कोडलाई जनाउने सामान्य शब्द।

- फिसिङ (Phishing): इमेल, एसएमएस, फोन, सामाजिक सञ्जाल वा सामाजिक इन्जिनियरिङ प्रविधि प्रयोग गरी पासवर्ड वा खाता नम्बरजस्ता संवेदनशील जानकारी खुलाउन प्रलोभन दिने आक्रमण।

- र्यान्समवेयर (Ransomware): तपाईंको डेटा इन्क्रिप्ट गरी फाइल वा नेटवर्कमा पुनः पहुँच दिनका लागि फिरौती माग्ने मालवेयर। यो हाल सबैभन्दा सामान्य आक्रमणमध्ये एक हो। डबल–जोखिम र्यान्समवेयरमा आक्रमणकारीले तपाईँको डेटा अनलाइन सार्वजनिक गर्ने धम्की पनि दिन्छ।

- अनलाइन सेक्सटोर्शन (Sextortion online): कसैको यौन व्यवहारसँग सम्बन्धित तस्बिर वा प्रमाण सार्वजनिक गर्ने धम्की दिई पैसा वा यौन फाइदा माग्ने कार्य।

- स्पुफिङ (Spoofing): आक्रमणकारीले आफूलाई चिनिएको वा विश्वासिलो स्रोत (जस्तै : साथी वा बैंक) का रूपमा प्रस्तुत गर्ने प्रविधि। यसमार्फत उनीहरूले सूचना चोरी, रकम ठगी वा उपकरणमा मालवेयर जस्ता हानिकारक सफ्टवेयर स्थापना गर्न सक्छन्।

यी आक्रमणहरू हुने आवृत्ति तपाईंको सङ्गठनको प्रकार र स्थानीय परिस्थितिको आधारमा धेरै फरक पर्न सक्छ। तर स्पुफिङ (Spoofing) मार्फत हुने ठगीको जोखिम सम्भवतः सबैभन्दा सामान्य हो जसको सामना तपाईंले गर्नसक्नुहुन्छ (जसलाई प्रायः व्यापारिक इमेल धोखाधडी – Business Email Compromise भनेर चिनिन्छ)। यो प्रायः त्यति बेला हुन्छ जब स्पुफ गरिएको इमेल वा सन्देशमार्फत पैसा स्थानान्तरण गर्न अनुरोध गरिन्छ र यसको मुख्य सुरक्षा प्राविधिक भन्दा प्रक्रियागत हुन्छ। तपाईंले यस्तो संस्कृति निर्माण गर्नुपर्छ जहाँ असामान्य अनुरोधहरूलाई सधैँ शङ्का गरेर हेरिन्छ र भुक्तानीको सही स्वीकृति प्रक्रियाहरू सधैँ कायम रहन्छन्।

सधैँ सम्झनुहोस्, ठगी र आक्रमणका नयाँनयाँ स्वरूपहरू निरन्तर विकसित हुँदैछन्। त्यसैले तपाईंको सङ्गठनलाई अपडेट राख्नु र नयाँ खतराहरूको प्रतिक्रिया स्वरूप आफ्ना मार्गदर्शनहरू नियमित रूपमा सुधार्नु अत्यन्त महत्वपूर्ण हुन्छ।

तपाईँको कर्मचारी: सबैभन्दा उच्च जोखिम र पहिलो सुरक्षा पङ्क्ति

डिजिटल प्रणालीहरूमा हुने धेरै ह्याकहरू प्रायः "मानव त्रुटि" का कारण हुन्छन्, जस्तै कसैले गल्तीले लिङ्क क्लिक गर्दा उनीहरूलाई नक्कली साइटमा पुर्‍याइन्छ। यस्ता स्क्यामहरू पत्ता लगाउन दिन–प्रतिदिन कठिन हुँदै गएको छ र कर्मचारीहरूलाई कुनै पनि अप्रत्याशित आउने सन्देश सम्भावित खतरनाक हुन सक्छ भनेर सोच्न प्रोत्साहित गर्नु पर्छ।

- सङ्गठनको आकार जे भए पनि, एउटा विश्वसनीय र प्राविधिक रूपमा सक्षम कर्मचारीलाई समग्र डिजिटल सुरक्षा जिम्मेवारी दिने व्यवस्था गर्नुहोस् र सुनिश्चित गर्नुहोस् कि उनीहरूले:
    - उपयुक्त तालिम पाएका छन् (नियमित अद्यावधिकसहित)।
    - घटना प्रतिक्रिया र पुन: प्राप्ति योजना लागू गरेका छन्, जसमा कम्तिमा:

  - सङ्गठनका लागि महत्वपूर्ण र आवश्यक प्रणालीहरू।
  - सहयोगका लागि कसलाई सम्पर्क गर्ने वा घटना रिपोर्ट गर्ने।

    - सम्बन्धित राष्ट्रिय CSIRT (Computer Security Incident Response Team) वा CERT (Computer Emergency Response/Readiness Team) को प्रोटोकलको विवरण जान्दछन्। यद्यपि यी सामान्यतया ठूलो संस्थाहरूका लागि तयार पारिएका हुन्, तर यसमा राम्रो सल्लाह र सुझावहरू उपलब्ध हुन्छन्।

    - सबै कर्मचारीलाई नयाँ–नयाँ खतराहरूको नियमित अद्यावधिक जानकारी साझा गर्छन्।

    - दोष लगाउने भन्दा खुला रिपोर्टिङको वातावरण प्रवर्द्धन गर्छन्।
    - साइबर सुरक्षा सम्बन्धी नियमित रिपोर्ट CEO/Board वा समान निकायलाई दिन्छन्।

- सबै कर्मचारीले आफ्ना सबै लगइन र एप्सका लागि जटिल र अद्वितीय युजरनेम र पासवर्ड प्रयोग गर्न सुनिश्चित गर्नुहोस्।
    - सबै पासवर्ड कम्तीमा १२ अक्षर लामो हुनुपर्छ र सम्भव भएसम्म सङ्ख्या, स–क्षर, ठूला अक्षर र प्रतीक प्रयोग गर्नुहोस्।
        - यी सम्झन गाह्रो भए पनि कागजी प्रतिलिपि बनाएर सुरक्षित ठाउँमा राख्नु उपकरणमा फोल्डरमा राख्नु भन्दा सुरक्षित हुन सक्छ।
        - पासवर्ड नियमित रूपमा अद्यावधिक गर्नुपर्छ र कुनै पनि डेटा चुहावटको घोषणा पछि तुरुन्त परिवर्तन गर्नुपर्छ।
    - पासवर्ड बनाउने अर्को वैकल्पिक तरिका भनेको तीनवटा अनियमित शब्द प्रयोग गर्नु हो, जस्तै apple, rift, ocean र ती शब्दहरूलाई जोडेर "appleriftocean" जस्तो एउटा पासवर्ड बनाउनु (फेरि पनि १२ अक्षरभन्दा लामो)।यस तरिकाले पासवर्ड याद गर्न सजिलो हुनु र पर्याप्त लामो हुनु दुवै फाइदा मिल्छ। साथै फरक–फरक प्रयोजनका लागि विविधता ल्याउन ती शब्दहरूको क्रम परिवर्तन गर्न सकिन्छ, जस्तै "oceanapplerift"।

- सङ्गठनसम्बन्धी र व्यक्तिगत जीवनसँग सम्बन्धित सबै लगइनहरूका लागि बहु–प्रमाणीकरण (multiple authentication) अनिवार्य गर्नुहोस्। कम्तीमा द्वि–प्रमाणीकरण (2FA) प्रयोग गर्नुपर्छ, जसको अर्थ दुई फरक प्रणाली वा कारक/श्रेणी प्रयोग गर्नु हो, जस्तै मोबाइल उपकरण र ल्यापटप, वा उपकरणमा पहुँच प्रमाणित गर्न अनुहार पहिचान (face recognition) को प्रयोग। MFA (Multi-Factor Authentication) भन्नाले बहु–कारक प्रमाणीकरण जनाउँछ। ध्यान दिनुहोस्, 2SV (Two-Step Verification) भनेको दुई चरणमा गरिने प्रमाणीकरण हो तर प्रायः एउटै प्रमाणीकरण श्रेणीभित्रका दुई चरण प्रयोग गरिन्छ।

ICT4D Collective

- द्वि–प्रमाणीकरण (Dual Authentication) सक्षम गर्नका लागि विभिन्न एपहरू उपलब्ध छन्, जसमा समावेश छन्:
    - Duo Mobile (Cisco)
    - Microsoft Authenticator
    - Google Authenticator

- साइबर सुरक्षासम्बन्धी वार्षिक तालिम तथा अद्यावधिक सबै कर्मचारीलाई उपलब्ध गराउनुहोस्, र उनीहरूलाई कार्यस्थलमा मात्र होइन, व्यक्तिगत जीवनमा पनि अनलाइन आफ्नो सुरक्षा र सुरक्षित व्यवहारप्रति जिम्मेवारी लिन प्रोत्साहित गर्नुहोस्।

- कर्मचारीहरूलाई कामसँग सम्बन्धित उपकरण र एपहरू व्यक्तिगत प्रयोजनका लागि प्रयोग गर्न अनुमति नदिनुहोस्।

- साथै कुनै कर्मचारी वा प्रयोगकर्ता सङ्गठनबाट बाहिरिँदा उनीहरूको सबै खाता निष्क्रिय वा समाप्त गरिएको सुनिश्चित गर्नुहोस् र उनीहरूसँग सम्बन्धित व्यक्तिगत डाटा तपाईँको प्रणालीबाट हटाइएको सुनिश्चित गर्नुहोस्।

- स्वयंसेवक र अस्थायी कर्मचारीहरू विशेष रूपमा जोखिमको स्रोत हुन सक्छन्, त्यसैले उनीहरूले तपाईँका लागि कुनै पनि काम सुरु गर्नुअघि पूर्ण रूपमा तालिम लिएको र तपाईँको साइबर सुरक्षा नीतिहरू अपनाएको सुनिश्चित गर्नुहोस्।

ICT4D Collective

डाटा सुरक्षा तथा व्यवस्थापन

डाटा कुनै पनि सङ्गठनका लागि जीवनरेखा हुन्, जसमा कर्मचारी, सेवाग्राही, साझेदार, तपाईँका सञ्जालहरू तथा सङ्गठनका गतिविधिसम्बन्धी जानकारी समावेश हुन्छन्। यी डाटासँग सम्बन्धित सुरक्षा र गोपनीयता कायम राख्नु अत्यन्त उच्च प्राथमिकता हुनुपर्छ। यस उद्देश्यका लागि तल उल्लेखित असल अभ्यासहरू अपनाउन सिफारिस गरिन्छ :

- ब्याकअप, फेरि ब्याकअप र अझै फेरि ब्याकअप गर्नुहोस्। महत्त्वपूर्ण डाटाका सुरक्षित धेरै प्रतिलिपिहरू राख्नुहोस्, ताकि तपाईँ ह्याक वा र्यान्समवेयर आक्रमणको सिकार भए पनि सजिलै पुनः काम सुरु गर्न सक्नुहोस्।
    - यसलाई क्लाउडमा राख्ने कि विभिन्न सुरक्षित हार्ड डिस्कहरूमा फरक–फरक स्थानमा (वा कागजमा पनि) राख्ने भन्ने निर्णय गर्नुहोस्।
        - फरक–फरक स्थानमा राख्नु महत्त्वपूर्ण हुन्छ, ताकि भौतिक चोरी, आगलागी, वा प्राकृतिक प्रकोप भए पनि डाटा सुरक्षित रहोस्।
    - कुनै एक सम्पूर्ण प्रणाली प्रभावित भएमा पनि डाटा सुरक्षित रहोस् भनेर फरक–फरक अपरेटिङ सिस्टम चल्ने उपकरणहरूमा ब्याकअप राख्ने विचार गर्नुहोस् (जस्तै, एउटा Windows मा र अर्को macOS वा Linux मा)।

- प्रत्येक विकल्पका फाइदा र बेफाइदाबारे विविध विचारहरू छन्, जुन धेरै हदसम्म तपाईँका प्राथमिकता र विशेषज्ञतामा निर्भर गर्दछ तर महत्त्वपूर्ण कुरा भनेको डाटा ब्याकअप गर्नु नै हो।

- तपाईँको देशमा डाटा व्यवस्थापन अभ्याससँग सम्बन्धित कानूनी स्थिति बुझ्नुहोस् र त्यसको पालन गर्नुहोस्।

    - यदि तपाईँको देशमा राष्ट्रिय नीति छैन भने, युरोपियन GDPR (General Data Protection Regulation) लाई उपयोगी मोडलको रूपमा पालन गर्न सकिन्छ।

- कम्तीमा कुनै व्यक्तिको व्यक्तिगत जानकारी/डाटा राख्न उनीहरूको अनुमति लिनुहोस्।
    - यदि अब त्यसलाई राख्न आवश्यक छैन भने सबै जानकारी मेट्नुहोस्।
        - नियमित रूपमा ती व्यक्तिसँग जाँच गर्नुहोस् कि उनीहरू तपाईँले डाटा राखिरहनुमा सन्तुष्ट छन् कि छैनन्।

- व्यक्तिहरूसँग सम्बन्धित निजी जानकारी सधैँ पासवर्डद्वारा सुरक्षित फाइलहरूमा र एन्क्रिप्ट गरिएको फोल्डरभित्र मात्र सुरक्षित रूपमा राखेर सुनिश्चित गर्नुहोस्।
    - र सबै पासवर्डको सुरक्षित अभिलेख राख्न सुनिश्चित गर्नुहोस्।

- स्टाफको पहुँच अन्य स्टाफ र क्लाइन्टको निजी डाटा (टेक्स्ट, तस्वीरहरू, अडियो, भिडिओ) मा आवश्यकताअनुसार मात्र सीमित गर्नुहोस्।

संस्थाको डिजिटल प्रणाली

संस्थाको डिजिटल प्रणालीलाई सामान्यतया तीनवटा अन्तरसम्बन्धित तत्वका रूपमा बुझ्न सकिन्छ: उपकरण, सफ्टवेयर र नेटवर्क।

उपकरणहरू

- केवल भरपर्दो स्रोतबाट हार्डवेयर किन्नुहोस्।
- सबै दोस्रो हाते उपकरणहरूलाई फ्याक्ट्री रिसेट गर्नुहोस्।
- नयाँ संस्करण जारी हुँदा तपाईँको अपरेटिङ सिस्टमहरू (सर्वसाधारण रूपमा Windows, macOS, वा Linux) अप्डेट गर्नुहोस्।
- सबै उपकरणहरूलाई भौतिक रूपमा सुरक्षित गर्नुहोस्।

  - भौतिक तोडफोड डेटा हराउने सामान्य कारण हो र हार्डवेयर प्रतिस्थापन महङ्गो पर्छ।
  - यदि तपाईँको मोबाइल उपकरण चोरी भयो भने, सकेसम्म छिटो रिमोट्ली सबै डेटा मेटाउने व्यवस्था गर्नुहोस्। Android का लागि Find My Device एप वा iPhone का लागि Find My iPhone एप प्रयोग गर्नुहोस्। ध्यान दिनुहोस् कि उपकरण हराउनु अघि यी एपहरू सक्रिय राखिएको हुनुपर्छ।

- USB स्टिकको प्रयोग गरेर उपकरणहरू बीच डेटा स्थानान्तरण गर्न अनुमति नदिनुहोस्।

- पावर सर्जका कारण हुने क्षतिबाट तपाईँको विद्युत सर्किटलाई सुरक्षित राख्न सर्किट ब्रेकर प्रयोग गर्नेबारे विचार गर्नुहोस्।

- "स्मार्ट" उपकरणहरूको प्रयोग सीमित गर्नुहोस्। यस्ता उपकरणहरूले सामान्यतया तपाईँको प्रयोग ट्र्याक गर्न सक्छन् र सम्भावित कमजोर स्थान को स्रोत हुन सक्छन्।

सफ्टवेयर

- उच्च गुणस्तरको एन्टिभाइरस सफ्टवेयर प्रयोग गर्नुहोस् र उपकरणहरू नियमित रूपमा स्क्यान गर्नुहोस्।
  - राम्रो एन्टिभाइरस सफ्टवेयर निःशुल्क उपलब्ध छन् (उदाहरण: Avast, AVG, Avira, Bitdefender, McAfee, Norton, Sophos – छनोट तपाईँको अपरेटिङ सिस्टम अनुसार फरक पर्न सक्छ) ।
  - सुनिश्चित गर्नुहोस् कि यसमा एन्टिभाइरस, वेब सुरक्षा, र्यान्समवेयर सुरक्षा, र हानिकारक ट्राफिक रोकथामक्षमताहरू छन्।
  - सबै उपकरणहरूको पूर्ण स्क्यान नियमित रूपमा चलाउनुहोस् (साधारणतया महिनामा कम्तीमा एकपटक)।
  - नयाँ स्क्याम र ह्याकिङसम्बन्धी जानकारी दिने भरपर्दो स्रोतको सदस्यता लिन विचार गर्नुहोस् (अक्सर निःशुल्क)

  - Experian:https://www.experian.com/blogs/ask-experian/the-latest-scams-you-need-to-aware-of/
  - Ofcom:https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/top-tips-to-stay-safe-from-scammers/
  - Which:https://www.which.co.uk/news/article/the-latest-scam-alerts-from-which-aBRLy2b02Wk

- केवल भरपर्दो स्रोत वा विक्रेताबाट मात्र सफ्टवेयर किन्नुहोस्।
  - यदि तपाईँलाई यसलाई कसरी इन्स्टाल र प्रयोग गर्ने थाहा छ भने भरपर्दो ओपन सोर्स सफ्टवेयर प्रयोग गर्नुहोस्।
  - धेरै राम्रो निःशुल्क वा कम लागतका सफ्टवेयरहरू उपलब्ध छन् भन्ने कुरा सधैँ सम्झनुहोस्।
  - कहिल्यै पनि पाइरेटेड (अवैध) सफ्टवेयर प्रयोग नगर्नुहोस्।
    - यस्ता सफ्टवेयरमा हानिकारक (मालिसियस) कोड हुन सक्छ।
    - यस्ता सफ्टवेयर प्रायः पुराना हुन्छन् र नवीनतम सुरक्षा सुधारहरू समावेश नहुन सक्छन्।

- संस्थाभित्र अधिकांश प्रयोगकर्ताहरूलाई "प्रशासक अधिकार " नदिने व्यवस्था गर्नुहोस्, र सफ्टवेयर प्रयोगको पहुँच साँच्चिकै आवश्यक पर्ने व्यक्तिहरूमा मात्र सीमित गर्नुहोस् ।
  - न्यूनतम अधिकारको सिद्धान्त अपनाउनुहोस्, जसअनुसार अनावश्यक तथा उच्च जोखिमयुक्त अनुमति (जस्तै: एडमिन पहुँच) सीमित गरिन्छ, ताकि कुनै खातामा समस्या आएमा ठूलो क्षति हुन नपाओस्
  - प्रशासक प्रयोगकर्ता खाताहरू नियमित रूपमा निगरानी गर्नुहोस्, तिनीहरू ह्याक भएका वा दुरुपयोगमा परेका छैनन् भन्ने सुनिश्चित गर्न ।

ICT4D Collective

- नयाँ संस्करण उपलब्ध हुने बित्तिकै सफ्टवेयर सधैँ अपडेट गर्नुहोस् ।
    - यस्ता अपडेटहरूमा प्रायः प्रणालीलाई सुरक्षित राख्न सहयोग गर्ने सुरक्षा सुधारहरू समावेश हुन्छन् ।
- सबै प्रयोगकर्ताहरूले जटिल पासवर्ड प्रयोग गरिरहेका छन् भन्ने सुनिश्चित गर्नुहोस् ।
- संस्थाका उपकरणहरूमा प्रयोग गर्न पाइने एप्स तथा सफ्टवेयरहरू सीमित गर्नुहोस् ।
- माथि उल्लेख गरिएअनुसार सबै प्रयोगकर्ताहरूले जटिल पासवर्ड प्रयोग गरिरहेका छन् भन्ने सुनिश्चित गर्नुहोस् ।
- सङ्गठनका उपकरणहरूमा प्रयोग गर्न पाइने एप्स तथा सफ्टवेयरहरू सीमित गर्नुहोस्।
    - व्यक्तिहरूलाई सङ्गठनका उपकरणहरूमा आफ्नै सफ्टवेयर अपलोड वा स्थापना गर्न अनुमति नदिनुहोस्।

नेटवर्कहरू

- भरपर्दो इन्टरनेट सेवा प्रदायक, क्लाउड सेवा प्रदायक तथा प्रबन्धित सेवा प्रदायकको प्रयोग गर्नुहोस्।
    - ती सेवा प्रदायकहरूले डिजाइन चरणदेखि नै सुरक्षा समावेश गरिएका अभ्यासहरू स्पष्ट रूपमा अपनाएका छन् भन्ने सुनिश्चित गर्नुहोस्।
    - यसले सम्भावित आपूर्ति शृंखला सम्बन्धी जोखिमहरू सीमित गर्न मद्दत गर्दछ ।
- तपाईँका सबै राउटरहरू तथा कुनै पनि IoT (इन्टरनेट अफ थिङ्स) उपकरणहरू जटिल पासवर्डद्वारा सुरक्षित गरिएको छ र ती पासवर्डहरू नियमित रूपमा परिवर्तन गरिन्छन् भन्ने सुनिश्चित गर्नुहोस् ।
- पाहुनाहरूलाई इन्टरनेट पहुँच दिन आवश्यक परेमा, वाइफाइमा छुट्टै Guest Network (अतिथि नेटवर्क) सिर्जना गर्नुहोस्।

- ○ यसले तपाईँको मुख्य नेटवर्कलाई फायरवालको पछाडि अलग राख्न मद्दत गर्छ, जसले दुर्भावनापूर्ण (Malicious) आक्रमणहरूबाट नेटवर्कलाई सुरक्षित राख्न सहयोग पुऱ्याउँछ।

- तपाईँको वाइफाइ नेटवर्कका पासवर्डहरू भित्तामा, सूचना बोर्डमा वा सजिलै देखिने र फोटो खिच्न सकिने स्थानमा नराख्नुहोस् (दुर्घटनावश भए पनि) ।
- तपाईँका प्रणालीहरूमा हुने सबै बाह्य पहुँचहरू VPN (भर्चुअल प्राइभेट नेटवर्क) मार्फत मात्र हुने व्यवस्था गरिएको छ भन्ने सुनिश्चित गर्नुहोस्।

तपाईँको वेबसाइट

तपाईँको वेबसाइट संसारसँगको तपाईँको झ्याल हो। तलका सल्लाहहरूले तपालाई सुरक्षित रूपमा उपस्थित रहन मद्दत गर्नेछन्:

- सम्झनुहोस् कि तपाईँको वेबसाइटमा भएको सबै सामग्री नक्कल गरी वेबमा अन्यत्र प्रयोग गर्न सकिन्छ।
  - तपाईँके देखाउन चाहनुहुन्न ?
- तपाईँको वेबसाइट होस्ट गर्न भरपर्दो र सुरक्षित सेवा प्रदायक प्रयोग गर्नुहोस्।
- तपाईँको वेबसाइटमा भएको डाटाको नियमित रूपमा ब्याकअप लिनुहोस्।
- तपाईँको साइटमा कुन तस्बिर देखाउने भन्ने स्पष्ट नीति बनाउनुहोस् र त्यसको पालना सुनिश्चित गर्नुहोस्।

विशेष रूपमा विचार गर्नुहोस्:

- ▪ तपाईँ मानिसहरूको अनुहार देखाउन चाहनुहुन्छ कि उनीहरूलाई पहिचान गर्न सकिने अवस्था दिन चाहनुहुन्छ ?
- ▪ यो विशेष गरी संवेदनशील बालबालिका वा वयस्कहरूसँग काम गर्दा अत्यन्तै महत्त्वपूर्ण हुन्छ।

सम्भव भएसम्म SSL (Secure Sockets Layer) प्रमाणपत्र प्राप्त गर्नुहोस्, जसले साधारण http को सट्टा सुरक्षित हाइपरटेक्स्ट ट्रान्सफर प्रोटोकल (https) प्रयोग गर्न सक्षम बनाउँछ । https मा डाटा आदान–प्रदान गर्नुअघि ब्राउजर र सर्भरबीच सुरक्षित तथा इन्क्रिप्ट गरिएको जडान स्थापित गरिन्छ ।

- सम्भावित सुरक्षा कमजोरीहरू पहिचान गर्न आफ्नो वेबसाइटको नियमित रूपमा परीक्षण गर्नुहोस् ।
- डोमेन नाम/ठेगाना (URL) सकेसम्म छोटो तर अर्थपूर्ण राख्नुहोस्।
- स्वचालित कार्यक्रमहरूद्वारा ईमेल ठेगाना सङ्कलन (scrape) गर्न गाह्रो बनाउन, प्रत्यक्ष रूपमा ई–मेल ठेगानामा जाने लिङ्कहरू सामान्यतया प्रयोग नगर्नुहोस्।
    - सन्देशहरू तपाईंतर्फ निर्देशित गर्न सम्पर्क पृष्ठ (Contact Page) प्रयोग गर्नुहोस्।
        - आवश्यक परेमा CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) पनि प्रयोग गर्न सकिन्छ।
    - आफ्नो ईमेल ठेगानाको छवि (image) प्रयोग गर्नुहोस्।
    - वा a(dot)person(at)organisation(dot)org जस्तो ढाँचामा ई–मेल ठेगाना प्रस्तुत गर्नुहोस् ।
- केही संस्थाहरूले info@organisation.org जस्तो एउटै बाह्य सम्पर्क ई–मेल ठेगाना मात्र प्रयोग गर्न रुचाउँछन् ।
- आफ्ना सबै add-ons तथा plugins सधैँ अद्यावधिक (update) अवस्थामा राख्नुहोस् ।
- सामान्यतया वेबसाइटमा सामग्री तयार पार्ने र अपलोड गर्ने अधिकार सीमित सङ्ख्याका व्यक्तिहरूलाई मात्र दिनु उत्तम अभ्यास मानिन्छ।
    - सबै पहुँचसम्बन्धी प्रयोगकर्ता नाम (username) र पासवर्डहरू गोप्य तथा सुरक्षित रूपमा व्यवस्थापन गर्नुहोस्।
    - विभिन्न प्रकारका प्रयोगकर्ताहरूका लागि फरक–फरक सुरक्षा तहहरू प्रयोग गर्नुहोस् र प्रशासक (admin) खाताहरू एक वा दुईवटामात्र सीमित राख्नुहोस्।

- वेबसाइटसम्बन्धी कुनै पनि राष्ट्रिय निर्देशिका वा प्रतिबन्धहरू पालना गर्नुहोस्‌।
    - प्रयोगकर्ताको डाटा कसरी प्रयोग गरिन्छ भन्ने स्पष्ट गर्न तथा त्यसम्बन्धी विकल्पहरू प्रदान गर्न डाटा प्रयोग तथा कुकी (cookies—प्रयोगकर्तासम्बन्धी जानकारी सुरक्षित गर्न वेब सर्भरद्वारा प्रयोग गरिने फाइलहरू) नीतिहरू तयार पार्नेबारे विचार गर्नुहोस्‌।
- महङ्गो वेबसाइट डिजाइनमा अत्यधिक खर्च गर्न आवश्यक छैन, तर तपाईँले दिन चाहेको सन्देश स्पष्ट र सरल रूपमा प्रस्तुत हुने गरी डिजाइन राख्ने प्रयास गर्नुहोस्‌।
- यदि तपाईँको बजेटले अनुमति दिन्छ भने Vulnerability and Penetration Testing (VAPT) गर्ने विषयमा विचार गर्नुहोस्‌।

सामाजिक सञ्जाल

धेरैजसो नागरिक समाजका संस्थाहरूले आफ्नो कामको प्रचार गर्न र सेवाग्राहीहरूसँग जोडिन सामाजिक सञ्जालमा उपस्थिति राख्न चाहन्छन्, तर सामाजिक सञ्जाल प्रयोग गर्दा यससँग सम्बन्धित सुरक्षाजन्य जोखिमहरूबारे सधैँ सचेत रहनु आवश्यक छ।

- कुन–कुन सामाजिक सञ्जाल प्लेटफर्म प्रयोग गर्ने भन्ने विषयमा ध्यानपूर्वक विचार गर्नुहोस्, किनकि ती सबैले कुनै न कुनै रूपमा तपाईँबाट सङ्कलन गरेको डाटाबाट नाफा कमाउँछन्‌।
- आफ्नो संस्थालाई राम्रोसँग बुझ्ने र राम्रो तालिम प्राप्त गरेका अत्यन्तै थोरै व्यक्तिहरूलाई मात्र सामाजिक सञ्जाल खातामा सामग्री अपलोड गर्न अनुमति दिनुहोस्।
- सबै ठाउँमा जटिल प्रयोगकर्ता नाम (username) र पासवर्ड प्रयोग गर्नुहोस् (माथि उल्लेख गरिएका समान सुझावहरू हेर्नुहोस्)।
- सामाजिक सञ्जालका समूहहरूको सदस्यता विश्वासिला व्यक्तिहरूमा मात्र सीमित गर्नुहोस्।
    - उदाहरणका लागि फेसबुकमा समूहका नियमहरू प्रयोग गर्नुहोस् र सदस्य बन्नुअघि ती नियमहरूमा सहमति जनाउन लगाउनुहोस्‌।

ICT4D Collective

- सम्भव भएसम्म Signal जस्ता इन्क्रिप्टेड मेसेजिङ एपहरू प्रयोग गर्नुहोस्।
  - WhatsApp ले पनि सबै सन्देशहरूमा Signal को end-to-end encryption प्रयोग गर्छ।
  - यदि तपाईं Telegram प्रयोग गर्नुहुन्छ भने सधैं "Secret Chat" मोड प्रयोग गर्नुहोस्, तर त्यस अवस्थामा पनि end-to-end encryption केवल दुई जना सहभागीका लागि मात्र उपलब्ध हुन्छ।
- स्पष्ट अनुमति नदिइएसम्म कसैलाई पनि (कर्मचारी, सेवाग्राही वा आगन्तुकहरू समेत) तपाईँको गतिविधि वा कर्मचारीहरूको तस्बिर पोस्ट गर्न नदिनुहोस्।

इ-मेलहरू

इ-मेलहरू धेरै कमजोरीहरूको स्रोत हुन् र इ-मेल खाताहरूमा आक्रमण दिनहुँ बढ्दै गइरहेको छ।

- सबै कर्मचारीहरूलाई नियमित रूपमा ई–मेल सुरक्षासम्बन्धी स्मरणपत्रहरू प्रदान गर्ने तथा नयाँ प्रकारका जोखिम वा ठगी (माथि उल्लेखित अनुसार) बारे जानकारी प्राप्त हुनेबित्तिकै सूचना दिने प्रणाली कार्यान्वयनमा ल्याउनुहोस्।
- आफ्नो संस्थाबाट पठाइएको ई–मेलको जवाफ बाहेकका सबै आगमन ई–मेलहरू सम्भावित खतरा हुन सक्छन् भन्ने मान्यता राख्नुहोस्।
- कुनै पनि ई–मेलमा रहेको लिङ्क तबसम्म क्लिक नगर्नुहोस् जबसम्म त्यसको प्रामाणिकता र सुरक्षा पूर्ण रूपमा सुनिश्चित गरिएको हुँदैन। सुनिश्चित भएको अवस्थामा पनि एकपटक पुनः विचार गर्नुहोस्।
- सम्भव भएसम्म उच्चस्तरको सुरक्षा सुनिश्चित हुने गरी SPAM फिल्टरहरू प्रयोग गर्नुहोस्।
- DMARC (Domain Message Authentication Reporting) प्रयोग गर्नुहोस्।
- कुनै पनि ई–मेलप्रति शङ्का लागेमा, कर्मचारीहरूलाई ई–मेल खोल्नु अघि नै डिजिटल सुरक्षाको जिम्मेवारी सम्हाल्ने व्यक्तिसँग सम्पर्क गर्न प्रोत्साहित गर्नुहोस्।

- आगमन ई–मेलका लागि नियमहरू निर्धारण गर्नेबारे विचार गर्नुहोस्, जसअनुसार केवल विश्वासयोग्य सम्पर्कहरूबाट आएका ई–मेलहरू मात्र स्वीकार गरिन्छन्।
    - यसलाई सम्पर्क विवरण (माथि उल्लेखित अनुसार) सँग संयोजन गरी प्रयोग गर्दा अत्यन्त प्रभावकारी हुन सक्छ।
- धेरै व्यक्तिहरूलाई एउटै ई–मेल पठाउँदा सधैँ bcc (Blind Carbon Copy) प्रयोग गर्नुहोस्।
    - यसो गर्दा प्राप्तकर्ताहरूले एकअर्काको ई–मेल ठेगाना देख्न पाउँदैनन्।

निष्कर्ष

कुनै पनि प्रणाली १००% सुरक्षित हुनु कहिल्यै सम्भव हुँदैन। तथापि माथि उल्लेखित सल्लाहहरू पालना गर्दा साइबर सुरक्षासम्बन्धी घटनाका कारण तपाईँको संस्थामा पर्न सक्ने क्षतिको सम्भावना उल्लेखनीय रूपमा घटाउन सकिन्छ। अन्त्यमा, केही महत्त्वपूर्ण स्मरणहरू यस प्रकार छन्:

- कुनै न कुनै समयमा तपाईँको संस्था साइबर सुरक्षासम्बन्धी घटनाबाट प्रभावित हुन सक्ने सम्भावना उच्च छ भन्ने कुरा स्वीकार गर्नुहोस्।
- साइबर आक्रमणको प्रभाव न्यूनिकरण गर्न पूर्वतयारी योजना तयार राख्नुहोस्।
- डिजिटल सुरक्षाको जिम्मेवारी स्पष्ट रूपमा तोकिएको उपयुक्त व्यक्तिलाई जिम्मेवारी प्रदान गर्नुहोस्।
- स्वयंसेवक तथा अस्थायी कर्मचारीहरू सहित सबै कर्मचारीहरूलाई नियमित रूपमा साइबर सुरक्षासम्बन्धी अभ्यास र तालिम प्रदान गर्नुहोस्।
- सधैं जटिल पासवर्डहरू तथा बहु–तह प्रमाणीकरण (Multi-Factor Authentication) प्रयोग गर्नुहोस्।
- साइबर आक्रमणको सिकार भएमा यथाशीघ्र सहयोग खोज्नुहोस्।

परिशिष्टः पोस्टर वा तालिम कोर्सका लागि ग्राफिक्समा सजिलै प्रयोग गर्न सकिने सामग्री

स्रोत: Hive https://hivesystems.com/password

2024 मा ह्याकरले तपाईँको पासवर्ड ब्रुट फोर्स गर्न लाग्ने समय

ब्रुट फोर्स आक्रमणले ट्रायल–एण्ड–एरर विधि प्रयोग गरेर लगइन पहिचान, प्रमाणपत्र, र इन्क्रिप्सन कीहरू पत्ता लगाउने काम गर्छ। युजरनेम र पासवर्डको विभिन्न संयोजन प्रयोग गरिन्छ जबसम्म सही संयोजन फेला पर्दैन। कम्प्युटरहरूले यो प्रक्रिया धेरै छिटो गर्न सक्छन् र भविष्यमा क्वान्टम कम्प्युटरहरूले यसलाई अझ छोटो समयमा गर्न सक्नेछन्। यसरीका खतराहरू घटाउन बहु–प्रमाणीकरण (multiple authentication) विधिहरू प्रयोग गर्नु अत्यावश्यक छ।

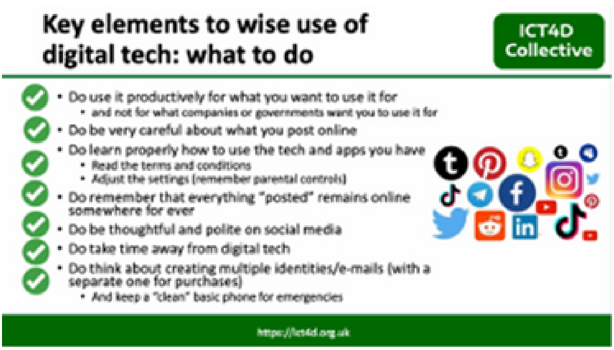
स्रोत: ICT4D Collective

तीन उदाहरणहरू विविध स्रोत सामग्रीका, जुन मुख्य रूपमा UKRI GCRF द्वारा वित्त पोषित MIDEQ परियोजनामा हाम्रो कामको क्रममा र त्यसपछि विकास गरिएको हो (हाम्रो प्रवासन र डिजिटल प्रविधि सम्बन्धी काम हेर्नुहोस्) ।

- यी स्लाइडहरू सजिलै प्रिन्ट गरेर कार्यालयको भित्तामा पोस्ट गर्न सकिन्छ, सरल सम्झाउने संकेतका रूपमा।

- डिजिटल प्रविधिको सुरक्षित, बुद्धिमानीपूर्ण र सुरक्षित प्रयोग सम्बन्धी विभिन्न विषयमा ग्राफिक्ससहितको पूर्ण स्लाइड डेकहरू धेरै भाषामा उपलब्ध छन्: https://ict4d.org.uk/sws/

ICT4D Collective



थप स्रोतहरू

यीमध्ये अधिकांश विश्वसनीय, छोटो, स्पष्ट, र सजिलै पहुँचयोग्य मार्गनिर्देशनहरू हुन् जसले साइबर सुरक्षासम्बन्धी विशेष पक्षहरूलाई समेट्छन्; केही लामो मार्गनिर्देशनहरू विशेष रूपमा नागरिक समाजका संस्थाहरूको आवश्यकतासँग सम्बन्धित छन्।

- **Canadian Centre for Cyber Security (2024):** Mitigating cyber threats with limited resources: guidance for civil society, https://www.cyber.gc.ca/en/news-events/mitigating-cyber-threats-with-limited-resources-guidance-civil-society
- **CISA (Cybersecurity and Infrastructure Security Agency, USA) (2024)**: Mitigating cyber threats with limited resources: guidance for civil society, https://www.cisa.gov/sites/default/files/2024-05/joint-guide-mitigating-cyber-threats-with-limited-resources-guidance-for-civil-society-508c_3.pdf
- **Civicus (2022):** Safety & cyber security: 8 tips for civil society digital defense,https://www.civicus.org/index.php/mediaresources/news/blog/6118-safety-cyber-security-8-tips-for-civil-society_digital-defense
- **Cloudflare (no date):** How to secure a website, https://www.cloudflare.com/en-gb/learning/security/how-to-secure-a-website/
- **Coulson, G. (Betterteam) (2024):** Cyber security policy overview and sample template, https://www.betterteam.com/cyber-security-policy
- **Crowdstrike (2024):** 12 most common types of cyberattacks, https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/

ICT4D Collective

- **GDPR.EU (2018):** What is GDPR, the EU's new data protection law?, https://gdpr.eu/what-is-gdpr/
- **Gov.UK (no date):** The National Cyber Security Centre, https://www.ncsc.gov.uk/
- **IT Force (no date):** 5 cybersecurity policies every medium-sized business needs, https://www.itforce.ca/blog/cybersecurity-policies-every-business-needs
- **National Democratic Institute (2022):** Cybersecurity Handbook for Civil Society Organizations, https://www.ndi.org/publications/cybersecurity-handbook-civil-society-organizations
- **Rubenking, N.J. (2024):** The best free antivirus software for 2024, PC Mag, https://uk.pcmag.com/antivirus/120817/the-best-free-antivirus-protection
- **Splunk (2023):** Top 50 Cybersecurity Threats, https://www.splunk.com/en_us/form/top-50-security-threats.html
- **Tom's Guide (2024):** The best encrypted messaging apps in 2024, https://www.tomsguide.com/reference/best-encrypted-messaging-apps
- **Workable (2024):** Company cyber security policy template, https://resources.workable.com/cyber-security-policy

ICT4D Collective

यो काम [Creative Commons – Attribution-ShareAlike 4.0 International License (CC BY-SA 4.0)](https://creativecommons.org/licenses/by-sa/4.0/) अन्तर्गत लाइसेन्स गरिएको छ। यस दस्तावेजको कुनै पनि भाग अनुमति बिना पुनः प्रयोग गर्न सकिन्छ, तर ICT4D Collective र लेखकहरूलाई श्रेय दिनु अनिवार्य छ।कृपया यस जानकारीलाई स्वतन्त्र रूपमा प्रयोग र साझा गर्न सक्नुहुन्छ, तर समावेश सबै कामहरूको कपीराइटको सम्मान गर्नुहोस् र कुनै पनि संशोधित संस्करण साझा गर्दा पनि श्रेय दिनुहोस्।