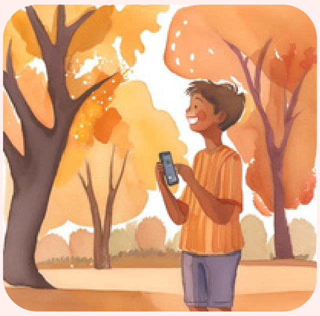
ऑनलाइन सुरक्षित रहा

amazon future engineer



दोन आठवड्यांपूर्वी, आदिलला त्याच्या वाढदिवसाला त्याचा पहिला स्मार्टफोन मिळाला... आणि त्याला तो खूप आवडला! तुम्ही त्याच्या ऑनलाइन प्रवासामध्ये सामील व्हाल का आणि त्याला ऑनलाइन सुरक्षा आणि गोपनीयतेबद्दल जाणून घेण्यास मदत कराल का?

आदिल छत्तीसगड,रायपूर येथे राहतोआणि आठवीत शिकतो. २०२४ मध्येतो १२ वर्षांचा झाला! त्याचा आवडताविषय भौतिकशास्त्र आहे - हे सर्वांना माहिती आहे! त्याला फुटबॉल खेळायला आवडते. त्याला ऑनलाइन खरेदीकरायला आवडते. त्याच्या फोनवर बोटांच्या अंतरावर या सगळ्या उत्साहजनक बाबीअसल्याने, त्याला माहितआहे की त्यालात्याचा फोन सुरक्षित ठेवण्याची आवश्यकता आहे, म्हणून तो पासवर्डसेट करण्याचा प्रयत्नकरत आहे.

पासवर्ड सुनिश्चित करतात की आपल्या परवानगीशिवाय कोणीही आपला फोन तपासू शकत नाही. जर आपल्या जवळचे नसलेले कोणी आपले फोटोस, संदेश, संपर्क आणि आपले सर्व रहस्ये पाहू शकेल, तर ते अस्वस्थ करणारे असते, बरोबर?

तुम्ही आदिलच्या पासवर्ड्सचा अंदाज लावू शकता का?

_ _ _ _ _ _ _ _

_ _ _ _ _ _ _ _

_ _ _ _

_ _ _ _ _

कदाचित् मी असे काहीतरी निवडेन, जे नक्की माझ्या आठवणीत राहू शकते!

माझा आवडता खेळ उपयुक्त ठरेल!

माझा जन्म वर्ष कोणालाच आठवणार नाही...

मला माझा फोन लवकर उघडता आला पाहिजे!

तुमचा पासवर्ड तुम्हाला लक्षात ठेवण्याइतका सोपा, पण इतरांना अंदाजलावायला कठीण असलापाहिजे! जर आदिलच्या पासवर्डचा अंदाज त्याच्याबद्दलच्या साध्यामाहितीवरून लावणे इतके सोपेअसेल, तर तो मजबूत असूशकत नाही!

मजबूत पासवर्ड सेट करणे

मजबूत पासवर्डची मार्गदर्शक तत्त्वे

अपरकेस आणि लोअरकेसमधील अक्षरे,आकडे आणि विशेष चिन्हे यांचे मिश्रण वापरा।

✗	✓
shirtsatninetyniners	$hirts@99Rs&

त्याला मोठे करा,८-१२ अक्षर, आकडे, चिन्हे वापरा

✗	✓
foot$	footballlover12

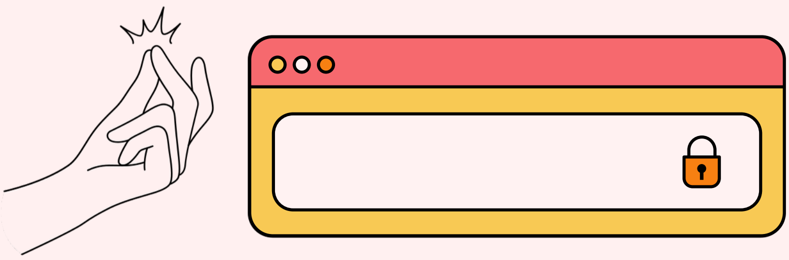
साधे, सहज अंदाज लावता येणारे शब्द वापरू नका।

✗	✓
adilraipur	h0lidaysandch0colat3

तुमचा वाढदिवस किंवा पाळीव प्राण्याचे नाव यासारखी साहजिक वैयक्तिक माहिती वापरणे टाळा।

✗	✓
bruno2012	dRjox76!$kL57

Forgot Password?



तुमच्या खात्यांपैकी एकासाठी एक मजबूत पासवर्डतयार करण्याकरिता तुम्ही हीच मार्गदर्शक तत्त्वे वापरू शकता का?

टिप।

वेगवेगळ्या खात्यांसाठी किंवा प्लॅटफॉर्मसाठी कधीही एकच पासवर्ड वापरू नका. यामुळे, कोणी जरी तुमच्या एका खात्यात प्रवेश करू शकले तरी ते दुसऱ्या खात्यांमध्ये लॉग इन करू शकणार नाहीत। अधिक सुरक्षित राहण्यासाठी, दर ३ महिन्यांनी किमान एकदा तुमचे पासवर्ड बदला.

ऑनलाईन गोपनीयता

amazon future engineer

आता आदिलनेत्याच्या सर्व खात्यांसाठी मजबूतपासवर्ड सेट केलेआहेत, त्यामुळे त्याला सुरक्षित वाटते पण त्याच्या एकूणऑनलाइन सुरक्षितता आणि त्याच्या हिताची खात्री करण्यासाठी मजबूतपासवर्ड पुरेसे आहेतका? त्याच्या ऑनलाइनआणि ऑफलाइन सवयींवरएक नजर टाका: तुम्हाला काही फरकजाणवतो का? इंटरनेट ब्राउझकरताना त्याने काहीगोष्टी लक्षात ठेवल्यापाहिजेत का?

आदिलच्या ऑफलाईन सवयी

आदिल त्याच्या मित्रांसह घरी येईपर्यंत वाट पाहतो आणि मग खाजगी विषयांवर चर्चा करतो जेणेकरून कोणीही चुकून ऐकू नये!

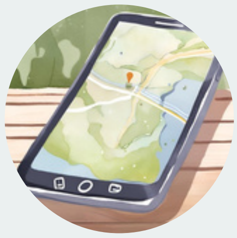
जर खेळाच्या मैदानावर कोणी आदिलला त्याच्या शाळेचे नाव किंवा पत्ता विचारला तर तो नम्रपणे सांगण्यास नकार देतो.

जर शाळेच्या फॉर्ममध्ये पालकांच्या बँक तपशीलांची मागणी केली तर तो नेहमीच ते का आवश्यक आहे ते तपासतो आणि कोड/पासवर्ड शेअर करत नाही.

पत्रे किंवा पार्सल उघडण्यापूर्वी, तो पाठवणारा कायदेशीर, सुरक्षित आहे आणि त्यांना त्याचा पत्ता कसा माहित आहे याची खात्री करतो.

आदिलच्या ऑनलाईन सवयी

आदिल खाजगी तपशील कोण पाहू शकते हे न पाहता टिप्पण्यांमध्ये चर्चा करतो.



आदिल त्याच्या पोस्टवर त्याचे लोकेशन टॅग करतो आणि अनेकदा ऑनलाइन त्याचे लोकेशन शेअर करतो.

नवीन आणि अपरिचित वेबसाइट्ससाठी साइन अप करताना, तो मागितलेली सर्व माहिती शेअर करतो.

तो अज्ञात लिंक्सवर मुक्तपणे क्लिक करतो, त्याला विश्वास आहे की लिंक्स त्याला नेहमीच अशा ठिकाणी घेऊन जातात जिथे त्याला अधिक रोमांचक गोष्टी सापडतील.

ऑनलाईन गोपनीयता

गोपनीयता म्हणजेतुमच्याबद्दल कोणाला कोणतीमाहिती आहे यावरनियंत्रण असणे.वेगवेगळ्या लोकांनावेगवेगळ्या पातळीच्या गोपनीयतेत सोयीस्कर वाटते - उदा. काही लोकांनात्यांचे वाढदिवस शेअरकरायला आवडत नाही, तर काहींना आवडते! तरीही, जसे आपणआपले ठिकाण किंवावैयक्तिक प्रसंग ऑफलाइनकोणालाही शेअर न करण्याची काळजीघेतो, तसेच ऑनलाइनजगात तुमची गोपनीयता राखणे आणि वाढवणेतुम्हाला सुरक्षित ठेवण्यास मदत करू शकते. आदिलला माहितीचे संरक्षणकरायला शिकून आपल्याऑफलाइन सुरक्षितता आणिगोपनीयतेच्या सवयी त्याच्या ऑनलाइन जीवनात रूपांतरित करण्यासमदत करा!

ऑनलाईन विचारल्या जाणाऱ्या माहितींचे प्रकार [2 3]

वैयक्तिक - म्हणजेच, अशी माहिती जी अनोळखी लोकांना प्रत्यक्ष किंवा अप्रत्यक्षपणे एखाद्या व्यक्तीची ओळख पटवण्यास मदत करू शकते - जसे की तुमचे नाव!

विशेषतः अज्ञात/असत्यापित प्लॅटफॉर्मवर ऑनलाइन शेअरिंग करणे टाळा, कारण त्याचे वापर तुमचे नुकसान करण्यासाठी केले जाऊ शकते.

संवेदनशील वैयक्तिकमाहिती- माहितीचा गैरवापर होण्याची शक्यता जास्त असते कारण ती इतर महत्त्वाच्या गोष्टी सांभाळून ठेवते - जसे की तुमची स्वाक्षरी!

इतरांबरोबर ऑनलाइन शेअर करू नका!*

बिगर-वैयक्तिक - म्हणजेच, अशी माहिती जी एखाद्या व्यक्तीची ओळख पटविण्यासाठी वापरली जाऊ शकत नाही! जसे कि आवडता रंग.

तुमच्या सोयीनुसार, वैयक्तिक माहितीशिवाय शेअर केले जाऊ शकते.

*जर तुम्हाला नेटबँकिंग, शॉपिंग किंवा सरकारी पोर्टलसारख्या ऑनलाइन सेवांसाठी संवेदनशील माहिती सादर करायची असेल, तर फक्त अधिकृत आणि चाचणी केलेल्या वेबसाइट वापरा आणि अधिकाऱ्यांशी बोला!

आदिलबद्दल माहितीची यादी खाली दिली आहे. मानसिकदृष्ट्या प्रत्येकाला योग्य श्रेणीत ठेवा: वैयक्तिक, बिगर-वैयक्तिक आणि संवेदनशील वैयक्तिक!

नांव

बोटांचे ठसे

शाळेचे नाव

समीक्षा आणि प्रतिसाद

सामान्य छंद

वय

पासवर्ड

घराचा पत्ता

ई-मेल पत्ता

बँक तपशील

1.San José Public Library.Toolkit: What is Online Privacy? www.sjpl.org/toolkit-what-online-privacy/.
2. Security Intelligence (IBM Security) (2023, July). Personal Data vs. Sensitive Data: What's the difference. www.securityintelligence.com/posts/personal-data-vs-sensitive-data-what-is-the-difference/
3. Aashish Aryan (2020, July). Explained: What is non-personal data? Indian Express. https://indianexpress.com/article/explained/non-personal-data-explained-6506613/.

सुरक्षा टूलकिट!

अभिनंदन! तुम्ही आदिलला ऑनलाइन सुरक्षितता आणि गोपनीयता युक्त्यांमध्ये प्रावीण्य मिळवण्यास मदत केली आहे. बक्षीस म्हणून, हजर आहे एक खास बॅकपॅक आहे... त्यातील सर्व प्रकारची छानशी साधने तुम्हाला आणि आदिलला ऑनलाइन अधिक सुरक्षित ठेवतील! ते काय आहेत ते पहायचे आहे का?

डबल सुरक्षा

तुमच्या खात्यांवर अतिरिक्त लॉक सेट करण्यासाठी २ फॅक्टर प्रमाणीकरण वापरा! याद्वारे हे सुनिश्चित होईल की जरी कोणी तुमच्या पासवर्डचा अंदाज लावला तरीही त्यांना प्रवेश करण्यासाठी दुसरा कोड आवश्यक असेल. कोणत्याही खात्यावरील सेटिंग्जमध्ये जाऊन गोपनीयता आणि सुरक्षा अंतर्गत त्यांना शोधा.

साईट चेकर

तुम्ही सुरक्षित आणि विश्वासार्ह वेबसाइटवर आहात याची काळजीपूर्वक खात्री करण्यासाठी या मार्गदर्शक तत्त्वांचा वापर करा.

> तुम्ही ब्राउझरवर ज्या वेबसाइटवर टाइप करता त्या वेबसाइटची लिंक तपासा,आणि ती “https” ने सुरू होत असल्याची खात्री करा

> लिंकचे नाव “.com” “.org” “.gov” किंवा “.edu.in” ने संपत असल्याची खात्री करा - ही मानक नावे आहेत

> वेबसाइट कोणी बनवली आणि ती कशी डिझाइन केली आहे हे समजून घेण्यासाठी संपूर्ण वेबसाइट - विशेषतः अबाउट(आमच्याबद्दल) सेक्शन - तपासा.

लिंक शील्ड

लिंक शील्ड अज्ञात किंवा संशयास्पद लिंक्सपासून दूर राहण्यास मदत करण्यासाठी येथे काही मार्गदर्शक तत्त्वे आहेत - त्त त्यावर क्लिक करु नका! जर तुम्हाला अनपेक्षित स्त्रोताकडून लिंक मिळाली, ती चुकीची दिसत असेल, त्यात स्पेलिंगच्या चुका असतील किंवा आकर्षक संदेश येत असेल, तर दूर राहा... कधीकधी, अज्ञात लिंक्स तुमची माहिती चोरु शकतात किंवा तुमच्या डिव्हाइसवर हानिकारक व्हायरस डाउनलोड करु शकतात.

प्रायव्हसी बडी

तुम्हाला माहिती आहे का? बहुतेक मेसेजिंग, गेमिंग आणि सोशल मीडिया प्लॅटफॉर्म तुम्हाला तुमचे प्रोफाइल इतरांपासून लपवण्याची आणि तुम्ही काय पोस्ट करता ते कोण पाहू शकते हे नियंत्रित करण्याची मुभा देतात! तुम्हाला मेसेज करण्याची परवानगी कोणाला आहे हे देखील तुम्ही नियंत्रित करू शकता आणि तुमच्या अकाउंट सेटिंग्जमधील गोपनीयता विभागातील पर्याय काळजीपूर्वक निवडून तुम्ही अधिक सुरक्षित राहू शकता!

उत्तर कुंजी

amazon future engineer

तुम्ही आदिलच्या पासवर्ड्सचा अंदाज लाऊ शकता का?

P A S S W O R D

F O O T B A L L

2 0 1 2

1 2 3 4 5

ऑनलाईन गोपनीयता

वैयक्तिक	बिगर-वैयक्तिक	संवेदनशील वैयक्तिक
नाव	समीक्षा आणि प्रतिसाद	पासवर्ड
वय	सामान्य छंद	बोटांचे ठसे
शाळेचे नाव		बँक तपशील
		घराचा पत्ता
		ई-मेलपत्ता