इंटरनेट सुरक्षा के लिए अक्सर पूछे जाने वाले प्रश्न

भाग 1: अपनी गोपनीयता और सुरक्षा का प्रबंध करें

1. अपना पासवर्ड कैसे ऑनलाइन सुरक्षित रखें ?

पासवर्ड साइबर अपराधियों के लिए पहली सुरक्षा रेखा होते हैं। यह महत्त्वपूर्ण होता है कि आप एक मजबूत पासवर्ड का चुनाव करें जो कि आपके हर जरूरी अकाउंट के लिए अलग हो, और नियमित समय पर अपने पासवर्ड को अपडेट करना एक अच्छी आदत होती है। एक मजबूत पासवर्ड बनाने के लिए और उसको सुरक्षित रखने के लिए निम्नलिखित सलाहों पर ध्यान दें –

अपने हर एक जरूरी अकाउंट जैसे कि इमेल और ऑन लाइन बैंकिंग के लिए एक अनोखे पासवर्ड का प्रयोग करें

अपने हर ऑन लाइन अकाउंट के लिए एक ही पासवर्ड का चुनाव करने का मतलब है अपने घर, आफिस और कार को एक ही ताले से लॉक करना – अगर अपराधी को एक पता लग जाता है तो, सभी जोखिम में आ जाते हैं। इस कारण जिस पासवर्ड का प्रयोग आप ऑन लाइन न्यूज लेटर के लिए करते हैं उसका उपयोग अपने ई मेल अथवा बैंक अकाउंट के लिए ना करें। अलग अलग पासवर्ड का चुनाव आपको सुरक्षित रखेगा।

एक लंबे पासवर्ड का प्रयोग करें जो कि नंबर, अक्षर और चिन्हों के साथ बना हो

जितना लंबा आपका पासवर्ड होगा, उसका अनुमान लगाना उतना ही मुश्किल होगा। इसलिए अपने पासवर्ड को लंबा रखिये ताकि आपकी जानकारी सुरक्षित रहे। नंबर, चिन्ह और मिक्स्ड केस अक्षरों का प्रयोग गुप्तचरों या बाकियों के लिए आपके पासवर्ड का अनुमान लगाना या उसे पता करना मुश्किल कर देगा। कृपया '123456' या 'पासवर्ड' का प्रयोग ना करें और सार्वजनिक रूप से उपलब्ध जानकारी जैसे कि आपका फोन नम्बर अथवा जन्मदिन अपने पासवर्ड में प्रयोग ना करें। यह ज़्यादा वास्तविक नहीं होता, और यह ज़्यादा सुरक्षित भी नहीं होता!

ऐसी वाक्यशैली का प्रयोग करने की कोशिश करें जिसे सिर्फ आप जानते हों

एक राय यह है कि ऐसी वाक्यशैली को सोचें जिसको सिर्फ आप जानते हों, और उसका संबंध किसी एक विशेष वेब साईट के साथ बनाये ताकि आप उसे याद रख सकें। अपने ईमेल के लिए आप इससे शुरू कर सकते हैं 'मेरे दोस्त शीतल और अक्षय एक दिन में एक बार मुझे एक मजाकियां ईमेल भेजते है' और फिर उसको उत्पन्न करने के लिए नम्बरों और अक्षरों का प्रयोग करें। "MfA&Ssmafe1ad" एक ऐसा पासवर्ड है जिसमें बहुत सारे परिवर्तन मौजूद है। फिर इस क्रिया को बाकी साइटों के लिए दोहराएँ।

अपने पासवर्ड के पुनः प्राप्ति के विकल्पों को सेट करें और उन्हें आधुनिक बनाए रखें

अगर आप अपने पासवर्ड को भूल जाएँ या लॉक आउट हो जाएँ, तो आपको अपने अकाउंट को दुबारा प्रयोग करने का रास्ता चाहिए। अगर आपको अपने पासवर्ड को दुबारा सेट करना है तो बहुत सी सेवाएँ आपको रिकवरी ईमेल एड्रेस पर ईमेल भेजेंगी, इसलिए यह सुनिश्चित करें कि आपका रिकवरी ईमेल एड्रेस आधुनिक हो और एक अकॉउंट जिसका आप प्रयोग कर सकें।

कभी कभी आप एक फोन नम्बर को भी अपनी प्रोफाइल में जोड़ सकते हैं ताकि पासवर्ड सेट करने के लिए आपको मेसेज के द्वारा एक कोड प्राप्त हो सके। अपने अकॉउंट पर अपना मोबाइल नम्बर होना, अपने अकाउंट को सुरक्षित रखने का सबसे आसान और भरोसेमंद तरीका है।

आपका मोबाइल नंबर रिकवरी ईमेल एड्रेस से या सुरक्षित प्रश्न से एक ज़्यादा सुरक्षित संकेत देने का तरीका है क्योंकि आपके पास अपने मोबाइल फोन पर भौतिक कब्जा होता है।

अगर आप फोन नम्बर को अकाउंट में नहीं डालना चाहते या नहीं डाल सकते, बहुत सी वेबसाईट आपको एक प्रश्न का चुनाव करने के लिए कहती हैं ताकि अगर आप अपना पासवर्ड भूल जाएँ तो आपकी पहचान सत्यापित हो सके। अगर आप कोई सेवा का प्रयोग कर रहे हैं जो आपको अपना प्रश्न बनाने की मंजूरी देती है, ऐसे प्रश्न का चुनाव करें जिसका जवाब सिर्फ आपको पता हो और ऐसा कुछ ना हो जिसको आपने सार्वजनिक रूप से पोस्ट किया है या जिसको आपने सोशल मीडिया पर दिखावा किया है।

एक ऐसा रास्ता ढूँढे जिससे आपका जवाब अनोखा पर यादगार बना रहे – आप ऐसा उपरोक्त सलाह के तहत कर सकते हैं – ताकि अगर कोई आपके जवाब का अनुमान लगा भी ले, वह उसको ठीक तरह से भर ना सकें। यह बहुत जरूरी है की आप जवाब को याद रखें – अगर आप उसे भूल गए तो हो सकता है आप आपने अकाउंट का दुबारा प्रयोग ना कर पाएँ।

2. कैसे अपने ई मेल अकाउंट को सुरक्षित रखें ?

यह सुनिश्चित करें कि जब तक आप ना चाहें आपका ईमेल आगे फॉरवर्ड या शेअर नहीं हो रहा है

अपनी ई मेल में फॉरवार्डिंग और डैलीगेशन सेटिंग को चेक करें। इनसे आपके अकाउंट के दूसरे लोग भी देख सकते हैं।

अगर आप अपना पासवर्ड भूल जाएँ, तो आपको अपने अकाउंट का दुबारा प्रयोग करने के लिए रास्ता चाहिए

अगर आपको आपने पासवर्ड को दुबारा सेट करना है तो आपको रिकवरी ईमेल ऐड्रेस प्राप्त हो सकता है, इसलिए यह सुनिश्चित करें कि रिकवरी ईमेल ऐड्रेस आधुनिक हो और एक ऐसा अकाउंट हो जिसका आप प्रयोग कर सकें। आप ई मेल अकाउंट में फोन नंबर भी डाल सकते हैं ताकि पासवर्ड को दुबारा सेट करने के लिए आपको मेसेज के द्वारा कोड प्राप्त हो सके।

आपने अकाउंट पर मोबाइल नंबर होना आपने अकाउंट को सुरक्षित रखने का सबसे आसान और भरोसेमंद तरीका है। आपका मोबाइल नंबर रिकवरी ई मेल ऐड्रेस या सुरक्षित रखने वाले प्रश्न से बेहतर सुरक्षित सूचना प्रदान करने वाला तरीका है क्योंकि, बाकी दोनों के जैसे, आपके पास आपने मोबाइल फोन का भौतिक कब्जा मौजूद होता है।

आपने अकाउंट के असामान्य प्रयोग या गतिविधि पर नजर रखें

आपने अकाउंट में असामान्य प्रयोग या संदेहजनक गतिविधि पर रोजाना **नजर** करें। आई पी ऐड्रेस की खोज के लिए पृष्ठ के सबसे नीचे 'डिटेल्स' लिंक पर क्लिक करें ताकि आपको पता चले कि आपके मेल का प्रयोग किसने किया है, और उससे सम्बंधित स्थान का पता चले। अगर आपको अपने अकाउंट में कोई संदेहजनक गतिविधि दिखती है तो तुरंत अपने पासवर्ड को बदलें और अपने अकाउंट से लॉग आउट कर लें।

जब आप आपने ई मेल में साइन इन कर रहे होते हैं, आपको यह जाँच कर सुनिश्चित करना चाहिए कि वेब ऐड्रेस https:// (and not just "http://") शुरू होता है। यह संकेत करता है कि आपका वेब साईट के साथ कनेक्शन इनक्रिप्टेड है और सुरक्षित है।

3. अपने डिवाइस को कैसे सुरक्षित रखें?

अगर आप रीडाइरैकट हो रहे हैं या पॉप अप एड्स, अनचाहे टूलबार, या अजीब नतीजे देख रहे हैं, हो सकता है आपके कंप्यूटर के अंदर मैलवेयर हो। मैलवेयर एक ऐसा सॉफ्टवेयर होता है जिसको तबाह करने के लिए और आपके कंप्यूटर पर नियंत्रण करने के लिए बनाया जाता है।

मैलवेयर के संकेत

अगर आपके कंप्यूटर में मैलवेयर मौजूद है, आप शायद यह लक्षण देखेंगेः

- पॉप–अप विज्ञापन
- अनचाहे टूलबार
- अनुचित खोज नतीजे या विज्ञापन
- जिस साईट का आप प्रयोग करना चाहते हैं वहाँ से रीडाइरैकट हो रहे हैं
- गलत सर्च इंजन दे नतीजे प्राप्त होना

अपने कंप्यूटर या ब्राउजर से मैलवेयर को हटाएँ

उन प्रोग्राम जिनको आप नहीं पहचानते उनकी जाँच करें, और अनइनस्टॉल करें।

जो बदलावों को आप देख रहे हैं उन्हें अनडू करने के लिए ब्राउजर रिसेट फीचर का प्रयोग करें और अपनी सेटिंग को वापिस साधारण कर लें। ऐंटिवायरस सॉफ्टवेयर का प्रयोग करें और अपने कंप्यूटर से मैलवेयर को हटा लें।

अपने ब्राउजर और ऑपरेटिंग सिस्टम को आधुनिक रखें।

ज़्यादतर ऑपरेटिंग सिस्टम जब अपग्रेड होते हैं तब आपको सूचित करते हैं – इन सूचनाओं को नजरअंदाज ना करें। सॉफ्टवेयर के पुराने वर्जनों में कभी कभी सुरक्षा की परेशानियाँ आती है जिस के कारण अपराधी आपके डेटा तक पहुँच सकते हैं।

किस चीज पर क्लिक करते हैं और क्या डाउनलोड करते हैं इस पर नजर रखें।

अनजाने आप एक लिंक पर क्लिक करते हैं जो आपके कंप्यूटर में मैलवेयर इंस्टॉल कर देता है। अपने कंप्यूटर को सुरक्षित रखने के लिए, सिर्फ उन लिंकों पर क्लिक करें या सिर्फ उन साइटों से डाउनलोड करें जिन पर आपको भरोसा है। किसी भी अनजान फाइल प्रकार को ना खोलें, या ब्राउजर में दिख रहे पॉप अप से प्रोग्राम को डाउनलोड ना करें।

सही प्रिंट विवरण और ऑटो–चेक्ड चेकबॉक्सेस पर भी डाउनलोड करते समय ध्यान दें। यह सुनिश्चित करें कि जो प्रोग्राम आप डाउनलोड कर रहे हैं उनको आप समझते हैं।

अगर हो शक, रोको तब

ई मेल, ट्वीट, पोस्ट, और ऑनलाइन विज्ञापन में मौजूद लिंक एक रास्ता होते हैं जहाँ से साइबर अपराधी आपके कंप्यूटर को संक्रमित करते है। अगर यह संदेहजनक लगता है, अगर आपको स्रोत का पता भी हो, बेहतर होगा उसे हटा दें।

कार्य करने से पहले सोचें

उन संदेशों से सावधान रहे जो आपको तुरंत कार्यवाही करने के लिए कहते हैं, कुछ ऐसा प्रदान करते हैं जो अविश्वसनीय हो, या आपकी निजी जानकारी की मांग कर रहे हों।

फिशर के हाथ ना लगें

फिशिंग का मतलब होता है जब आपको ई मेल या सोशल मीडिया मेसेज मिलता है जिसको देख कर लगता है कि वह एक वैध जगह से आ रहा है जैसे कि बैंक या सोशल नेटवर्किंग साईट। अगर आप मेसेज में एक लिंक पर क्लिक करते हैं, आप एक ऐसी वेब साईट पर पहुँच जाते हैं जो वैध लगती है पर हो सकता है असल में उसे अपराधी चला रहे हों और छल से आपको अपने यूजर नेम और पासवर्ड के साथ साइन इन करने के लिए कह रहे हो ताकि वह आपकी जानकारी पर कब्जा कर सकें। बेहतर होगा कि आप लिंक पर क्लिक ना करें इससे अच्छा ब्राउजर विंडो में वेब ऐड्रेस को टाइप कर लें और उस तरह साइट तक पहुँचें।

क्लिक करते समय सावधान रहे

नकली या दुर्भावनापूर्ण वेब साईट (या वैध जिनको अपराधियों द्वारा हैक कर लिया गया है) आपके डिवाइस और उस में मौजूद डेटा को खराब कर सकती हैं कभी कभी इनको 'ड्राइव बाये डाउनलोड्स,' भी कहा जाता है अगर आप उन का प्रयोग करें या साईट के लिंक पर क्लिक करें तो यह साईट दुर्भावनापूर्ण सॉफ्टवेयर आपके डिवाइस में इंस्टॉल कर सकती हैं। यह अक्सर वैध लगती हैं, कुछ ऐसा प्रदान करती हैं जो अविश्वसनीय हो या उसमें किसी तरह की अनुचित या गैरकानूनी सामग्री मौजूद हो सकती है।

भाग 2: ऑनलाइन घोटालों और खतरों से सुरक्षा

4. ऐसे कौन से कदम है जिनसे ऑनलाइन पहचान की चोरी से बच सकते हैं?

आम चालों को जान लेना जिनका अपराधी प्रयोग करते हैं वह आपको स्वयं को ऑन लाइन धोखों और पहचान की चोरी से बचाने मे मदद करेगा। यहाँ कुछ आसान सुझाव है :

- अगर कोई संदेहजनक मेल, तुरंत आया हुआ मेसेज या वेब पेज जो आपकी निजी जानकारी या वित्तीय जानकारी की मांग करता है, तो उसका जवाब ना दें।
- अगर आप एक ई मेल में या चौट में लिंक का पीछा करते हुए एक ऐसी साईट पर आये हैं जिस पर आपको भरोसा नहीं है तो उसमें कभी भी अपना पासवर्ड ना भरें।
- अपने पासवर्ड को ई मेल द्वारा ना भेजें, और दूसरों के साथ शेयर ना करें
- अगर आपको किसी जान पहचान के व्यक्ति से मेसेज आता है पर आपको लगता है कि यह बहरूपिया है तो यह हो सकता है कि उनके अकाउंट के साथ किसी साइबर अपराधी ने संक्रमित किया हो जो आपका पैसा या जानकारी आपसे निकालना चाहता हो। सावधानी से जवाब दें, या जवाब ना दें। आम चालों में यह शामिल है आपसे तुरंत पैसे की मांग करना, आपको ऐसा बताना की वह किसी और देश में हैं या यह कहना कि उनका फोन चोरी हो गया है इस लिए उन्हें फोन नही किया जा सकता। मेसेज आपको यह भी कह सकता है कि तस्वीर, लेख या विडियो देखने के लिए लिंक पर क्लिक करें, जो असल में आपको एक ऐसी साईट पर ले जाये जो आपकी जानकारी को चुरा सकती हो।

5. ऑनलाइन घोटालों से सुरक्षित कैसे रहें ?

वेब एक सर्वोत्तम स्थान हो सकता है, पर हर व्यक्ति जो ऑनलाइन है उसके इरादे नेक नहीं होते। यहाँ तीन आसान तरीके हैं जिससे आप धोखेबाजों से बच सकते हैं और वेब पर सुरक्षित रह सकते हैं

अनजान लोग जिनके पास तोहफे हैं उनसे सावधान रहे

अगर आपको कोई बताता है कि आप विजेता हैं और आपको अपनी निजी जानकारी के साथ एक फॉर्म भरने के लिए कहता हैं, लालच में आकर भरना मत शुरू कर दें। चाहे आप सबमिट बटन को क्लिक नहीं करते, फिर भी आप शायद अपनी जानकारी ठगों को प्रदान कर सकते हैं अगर आप अपनी जानकारी फॉर्म पर भरनी शुरू कर दें।

शोध करें

जब आप ऑनलाइन खरीददारी कर रहे हैं, बेचने वाले के बारे में शोध करें और कम कीमत होने के बारे में सावधान और सतर्क रहें, बिलकुल वैसे ही जैसे आप एक स्थानीय स्टोर पर होंगे। ऑनलाइन सौदों की ढँग से जाँच करें जो अविश्वसनीय लग रहा हो। किसी भी झाँसे में फँस कर नकली उत्पादों को ना खरीदें।

जब शक हो, सुरक्षित चलें।

क्या आपको किसी ऐड या प्रस्ताव के बारे में शंका उठ रही है? अपने अंतरमन पर भरोसा करें! सिर्फ उन्ही एड्स पर क्लिक करें या उन्ही उत्पादों को खरीदें जिनकी साइट सुरक्षित हों, जिनकी समीक्षा की गयी हो और जिन पर आपको भरोसा हो।

भाग 3: पारिवारिक सुरक्षा के मूलभूत आधार

6. माता पिता होने पर, कैसे सुनिश्चित करें कि हमारा बच्चा ऑनलाइन सुरक्षित हो?

व्यस्त माता पिता के लिए, यह कुछ व्यावहारिक सुझाव हैं जिससे आप अपने परिवार को ऑनलाइन सुरक्षित रख सकते है:

पासवर्ड को सुरक्षित रखें

अपने परिवार के पासवर्ड सुरक्षित रखने की जानकारी प्राप्त करने में मदद करें। अपने परिवार को याद दिलाते रहे कि अपने पासवर्ड को किसी भरोसेमंद बड़े जैसे कि माता पिता के अलावा किसी को नहीं बताना। यह सुनिश्चित करें कि जब वह सार्वजनिक कंप्यूटर का प्रयोग कर रहे हैं जैसे कि स्कूल में, किसी कैफे या लाइब्रेरी में तो उन्हें साइन आउट करने की आदत हो।

प्राइवसी सेटिंग और शेयरिंग कण्ट्रोल का प्रयोग करें

विचारों, तस्वीरों, वीडियो, स्टेटस अपडेट और भी बहुत कुछ शेयर करने के लिए बहुत सारी साइटें मौजूद हैं। कई सेवाएँ प्राइवेसी सेटिंग और कंट्रोल प्रदान करती हैं जो आपके यह फैसला करने में मदद करती हैं कि कौन आपकी जानकारी को देख सकता है जब आप उसे पोस्ट करते हैं। परिवार और दोस्तों की निजी जानकारी को गुप्त रख के उन्हें दूसरों की प्राइवेसी का सम्मान करने में मदद करें और लोगों को सार्वजनिक रूप से शेयर की गयी जानकारी में नाम से ना पुकारें।

उम्र प्रतिबंध को जाँचें

बहुत सी ऑनलाइन सेवाओं में उम्र प्रतिबंध मौजूद होते हैं जो यह देखते हैं कि उनकी सेवाओं का प्रयोग कौन कर रहा है। जैसे कि, आपको एक विशिष्ट ऑनलाइन अकाउंट के लिए किसी उम्र की आवश्यकता हो सकती है, और कुछ उत्पाद 18 साल या उससे कम के लिए प्रतिबंधित होते हैं। अपने बच्चे को अकाउंट के लिए साइन अप करने की मंजूरी देने से पहले हमेशा वेब साईट की नियमों और शर्तों को जाँचें, और अगर आपके पास परिवार के नियम मौजूद हैं कि कौनसी साईट का प्रयोग करना है और कौन सी नहीं तो हमेशा अपने बच्चों के साथ स्पष्ट बात करें।

अपने परिवार को जिम्मेदारी से संवाद करना सिखाएँ

यह एक अच्छा नियम हैः अगर आप यह किसी के मुँह पर नहीं कहेंगे, तो ऐसी टिप्पणी पोस्ट, मेसेज, ई मेल, इंस्टेंट मेसेज या किसी के पृष्ठ पर ना करें। इस चीज के बारे में बात करें कि जो आप ऑनलाइन लिखते हैं उसे दूसरा व्यक्ति कैसा अनुभव करेगा, और किस तरह का संवाद ठीक है इस बारे में परिवार में सलाह करें।

दूसरे वयस्कों और माहिरों से बात करें

अपने दोस्तों, परिवार जनों, अध्यापक, कोच और काउंसलर से बातचीत करें। अन्य माता पिता और विशेषज्ञ जो बच्चों के साथ काम करते हैं वह एक अच्छा स्रोत है जो आपकी यह जानने में मदद कर सकते हैं कि आपके परिवार के लिए क्या सही है, खास करके अगर आप एक ऐसे टेक्नोलॉजी के क्षेत्र का सामना कर रहे हैं जिसके बारे में आपको ज्ञान नहीं है।

अपने कंप्यूटर और पहचान को सुरक्षित रखें

ऐंटिवायरस सॉफ्टवेयर का प्रयोग करें और नियमित समय पर अपडेट करें। अपने परिवार के साथ निजी जानकारी की किस्मों के बारे में बात करें – जैसे की सोशल सिक्योरिटी नम्बर, फोन नम्बर या घर का पता – जिसको ऑनलाइन पोस्ट नहीं करना चाहिए। अपने परिवार को यह सिखायें कि अनजान लोगों द्वारा भेजी गयी अटैचमेंट या फाइलों को स्वीकार ना करें।

जारी रखें

सुरक्षित रहना एक समय की बात नहीं है – टेक्नोलॉजी में विकास होता है, इसके साथ ही आपके परिवार कि जरूरतें भी बढ़ेंगी। यह सुनिश्चित करें कि आप आपस में बातचीत करते रहे। अपने परिवार के बुनियादी नियमों को फिर से स्थापित करें, हर किसी के विकास को जाँचें और बात चीत करने के लिए नियमित अंतराल सेट करें। निम्नलिखत सलाहें आम मुद्दों को दर्शाती हैं जिसके बारे में माता पिता चिंता करते हैं।

7. कैसे मैं अपने बच्चों को साइबर बदमाशी के बारे में शिक्षित करूँ?

साइबर बदमाशी एक समय पर किया गया संवाद नहीं है, जब तक इसमें मौत का खतरा या शारीरिक तौर पर कोई विश्वसनीय खतरा मौजूद ना हो। बच्चों को तभी पता चलता है जब वह इसे देखते हैं, जबकि माता पिता असभ्य और शर्मनाक पोस्टों से ज़्यादा बच्चों द्वारा प्रयोग की गयी खराब भाषा के बारे में ज़्यादा फिक्रमंद होते हैं।

यह जरूरी है कि बच्चों को यह समझाया जाये कि बदमाशी क्या होती है ताकि अगर उनके साथ कोई बदमाशी कर रहा हो उन्हें तो यह पता रहे कि क्या करना है। बदमाशी नीचता और ड्रामे से भी आगे है – उसका मकसद नुक्सान पहुँचाना होता है और यह बार बार डराने वाला और आक्रामक व्यवहार होता है। बच्चों के साथ इस फर्क के बारे में बात करना अनिवार्य है। निम्नलिखत कुछ संकेत हैं जो हर किसी को अपने बच्चों से बात करते समय अपने दिमाग में रखने चाहिए।

यह सुनिश्चित करें कि बच्चों को इस बारे में जानकारी हो कि क्या करना है और अगर उनके साथ कोई बदमाशी करे तो कैसे जवाब देना है।

बच्चों को इस बात के लिए समझाना चाहिए कि तुरंत कुछ ना करें ना ही बदला लें बल्कि माता पिता, अध्यापक या किसी भरोसेमंद व्यक्ति से बात करे ताकि कोई यह परेशानी हल करने में उनकी मदद कर सके।

दर्शक नहीं कर्ता बनें

जबकि ज़्यादातर बच्चे बदमाशी में भाग नहीं लेते, पर कुछ इस चीज को अनुभव करते हैं। बच्चों से इसके महत्त्व के बारे में बातचीत करें – जब स्कूल या ऑनलाइन बदमाशी की बात आती है तो उन्हें केवल दर्शक ना बनने दें। गरिमा, सहानुभूति, और मतभेद का सम्मान करने की महत्त्वता पर जोर दें, और मुश्किल स्थितियों में बोलने के लिए उन्हें प्रेरित करें।

उन्हें पासवर्ड ना शेयर करना सिखायें

साइबर बदमाशी का एक आम भाग है जब बच्चे किसी और बच्चे के इ मेल या सोशल नेटवर्किंग अकाउंट में लॉग इन कर लेता है और नकली मेसेज और शर्मनाक पोस्ट भेज देता है। छोटी उम्र में यह कहें कि पासवर्ड गोपनीय होते हैं और सिर्फ माता पिता के साथ शेयर किये जाने चाहिए यह सीख कर बच्चे इस चीज से बच सकते हैं।

जिम्मेदारी, सम्मान से भरे ऑनलाइन व्यवहार की शिक्षा दें

व्यवहार का एक ऐसी नीति बनाएं जो आप चाहते हैं आपका बच्चा अपनायें (और समय समय पर इसे सुनिश्चित करने के लिए जाँच करें)। अगर वह देखते हैं कि दूसरे बदमाशी का सामना कर रहे हैं तो दूसरों के साथ खड़ा होना चाहिए क्योंकि साथी जब एक दूसरे के लिए खड़े होते हैं तो बदमाश को सबक सिखाने का यह सबसे असरदार तरीका होता है।