DRF

DigitalRightsFoundation

"KNOW YOUR RIGHTS"

ڈیٹا پرائیویسی کا کتابچہ

کتابچہ برائے اخفائے معلومات

Supported by

FRIEDRICH NAUMANN FOUNDATION For Freedom.

Pakistan

ہمارے بارے میں جانئے

ڈیجیٹل رائٹس فاؤنڈیشن ایک پاکستانی رجسٹرڈ غیر سرکاری تحقیقی ایڈووکیسی تنظیم ہے۔ اسے 2012 میں قائم کیا گیا اور یہ انسانی حقوق، شمولیت، جمہوری طریقہ ہائے کار اور ڈیجیٹل انتظام کار کی معاونت کے لیے آئی سی ٹیز پر زور دیتی ہے۔ ڈیجیٹل رائٹس فاونڈیشن آن لائن آزادانہ بات کرنے کے حق، ذاتی معلومات کے اخفا، ڈیٹا کے تحفظ اور عورتوں پر آن لائن تشدد جیسے امور کے حوالے سے کام کرتی ہے۔ ڈیجیٹل رائٹس فاونڈیشن آن لائن یا عملی طور پر کسی خاص یا ہر طرح کی آن لائن سنسر شپ اور انسانی حقوق کی خلاف ورزی کی مخالفت کرتی ہے۔

مزید معلومات کے لیے دیکھئے:

www.digitalrightsfoundation.pk

Supported by

FRIEDRICH NAUMANN FOUNDATION For Freedom.
Pakistan

DRF
DigitalRightsFoundation
"KNOW YOUR RIGHTS"

وضاحت:

اس اشاعت میں درست ترین مواد پیش کرنے کی پوری کوشش کی گئی ہے۔ مصنف یا ادارہ کسی بھی بھُول چوک کی ذمہ داری قبول نہیں کرتا کیونکہ ایسا دانستہ نہیں کیا گیا۔ بہرحال اگر ہمیں اپنے کام میں بہتری کے لئے درست معلومات مہیا کی جائیں تو ہم شکر گزار ہوں گے۔ فریڈرک نومن فاونڈیشن فار فریڈم کا اس کتاب میں دی گئی آراء سے متفق ہونا ضروری نہیں۔ اشاعت کا مواد ڈیجیٹل رائٹس فاؤنڈیشن کی ذمہ داری ہے۔

فہرست مضامین

پس منظر

اقوام متحدہ کنونشن برائے حقوق طفلاں کے مطابق بچے محض اشیاء نہیں ہیں جو والدین کی ملکیت مانے جائیں اور جن کے لیے فیصلے کیے جائیں، نہ ہی وہ زیر تربیت نابالغ افراد ہیں۔ اس کے بجائے وہ حقوق کے حامل انسان اور افراد ہیں۔

کنونشن میں بچپن اور لڑکپن میں فرق کیا گیا ہے جب کہ بچپن اٹھارہ برس کی عمر تک باقی رہتا ہے۔ یہ قانونی طور پر محفوظ شدہ اور سماجی طور پر تسلیم شدہ مدت ہے جس میں بچوں کو وقار کے ساتھ پھلنے پھولنے، سیکھنے، کھیلنے، ترقی کرنے اور نمو پانے کی اجازت ہونی چاہئے۔ یونیسف تسلیم کرتی ہے کہ ڈیجیٹل ٹیکنالوجی ایسا مظہر ہے جس نے جدید دور میں 'بچپن' کے معنی کو بدل کر رکھ دیا ہے۔ یونیسف کے مطابق جدید دور میں بچوں کو اپنے حقوق کے حوالے سے نئے خطرات کا سامنا ہے لیکن انھیں نئے مواقع بھی حاصل ہیں جنھیں وہ اپنے حقوق کے حصول کے لیے بروئے کار لا سکتے ہیں۔

انٹرنیٹ ایک وسیع و عریض جگہ ہے جسے دنیا بھر میں لوگ مختلف مقاصد کے لیے استعمال کرتے ہیں۔ بچوں کے لیے اس میں اس حوالے سے بہت کشش ہے کہ وہ زندگی میں ہر شے کے لیے تجسس رکھتے ہیں۔ انٹرنیٹ آپ کو علم اور تفریح فراہم کرتا اور دنیا بھر میں بہت سے صارفین سے آپ کو رابطے میں رکھتا ہے۔ انٹرنیٹ کے استعمال نے عالمی برادری کو ایک دوسرے کے زیادہ قریب کر دیا ہے۔ لیکن انٹرنیٹ کے استعمال کا ایک منفی رخ بھی ہے۔ جب لوگ انٹرنیٹ استعمال کرتے ہیں تو وہ دنیا بھر میں مختلف صارفین اور کمپنیوں کے ساتھ اپنے بارے میں معلومات کا تبادلہ کرتے ہیں۔ یہ معلومات مختلف صورتوں میں ہو سکتی ہیں اور انھیں اکٹھا کرنے کے مختلف

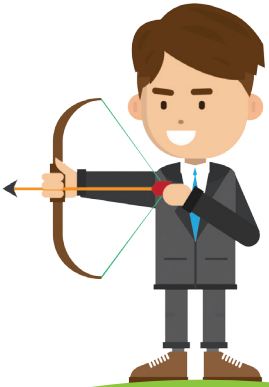
مقاصد ہو سکتے ہیں۔ دنیا بھر میں صارفین معلومات پیدا کرنے والی فیکٹریوں کی طرح کام کرتے ہیں۔ وہ معلومات تیار کرتے اور انھیں ہر روز ویب پر دوسروں سے بانٹتے ہیں۔ یہ معلومات ایسے انداز میں استعمال کی جاتی ہیں اور ان کا تجزیہ کیا جاتا ہے کہ ان کی بنیاد پر دنیا بھر میں انٹرنیٹ کے صارفین کے رویوں کے بارے میں پیشین گوئیاں ممکن ہو جاتی ہے۔

پاکستان میں انٹرنیٹ کے صارفین معلومات پیدا کرنے والی فیکٹریاں ہیں۔ وہ معلومات اور رویوں کو سامنے لاتے ہیں تاکہ کمپنیاں ان کا تجزیہ کریں۔ کمپنیاں اس ڈیٹا کو استعمال کرتے ہوئے اپنی سہولتوں کو بہتر بناتی ہیں اور آنے والے مارکیٹ کے رجحانات کے بارے میں پیشین گوئیاں کرتی ہیں۔ ایسی کمپنیاں بھی ہیں جو ان معلومات کو غیر اخلاقی مقاصد کے لیے استعمال کرتی ہیں اور بعض اوقات وہ ان معلومات کو صارفین کی اجازت کے بغیر کسی اور کو فروخت بھی کر دیتی ہیں۔

اس تناظر میں یہ بہت اہم ہو جاتا ہے کہ بچوں کو ذہنی طور پر تیار کیا جائے کہ وہ اپنی پرائیویسی کی حفاظت کر سکیں۔ والدین کو چاہئے کہ وہ ڈیجیٹل ٹیکنالوجی کے استعمال سے بچوں کو روکنے کے بجائے انھیں اس حوالے سے باشعور کرنے میں مدد کریں۔ ہم بچوں کے حقوق سے متعلق اقوام متحدہ کے کنونشن میں بیان کردہ حقوق کو من و عن تسلیم کرتے ہیں اور اخفائے معلومات سے متعلق اس کتابچے کا مقصد بچوں میں اس حوالے سے آگاہی پیدا کرنا ہے۔

مقاصد اور وظائف

اس کتابچے کے ذریعے ہمارا مقصد بچوں اور نوجوانوں کو اس طور تیار کرنا ہے کہ وہ ڈیجیٹل دنیا میں اپنی پرائیویسی کی حفاظت کر سکیں۔ ایسے دور میں جب حتیٰ کہ بالغ افراد بھی ڈیجیٹل دنیا کے منفی روپ سے محفوظ نہیں ہیں، یہ بہت اہم ہے کہ ہم ایسے اقدامات کریں جن سے ہمارے بچوں اور نوجوان اپنے ذاتی ڈیٹا کے ممکنہ غلط استعمال سے محفوظ ہو سکیں۔



خلاصہ

ہم نے کوشش کی ہے کہ سادہ زبان میں وضاحت کی جائے کہ ڈیٹا اور پرائیویسی سے کیا مراد ہے، ڈیٹا کی حفاظت کا کیا مطلب ہے اور کیوں یہ سب باتیں اہم ہیں؟ ہم نے یہ کوشش بھی کی ہے کہ سرکاری اور نجی دائرہ کار میں بھی فرق کو واضح کیا جائے اور یہ بھی کہ کیسے کسی فرد کا ڈیٹا خود اسی کے خلاف استعمال ہو سکتا ہے؟ سب سے آخر میں اپنے ڈیٹا کی حفاظت کے لیے چند اہم نکات بتائے گئے ہیں۔

والدین سے متعلق حصے میں ڈیٹا کی حفاظت کے لیے بچوں کو باشعور کرنے میں والدین یا قانونی سرپرستوں کے کردار اور فرائض سے متعلق وضاحت کی گئی ہے۔ ہمارے طریقہ کار کی بنیاد اس نکتہ پر ہے کہ بچے والدین کی ملکیت نہیں ہوتے اور اس لیے انھیں بچوں کی حفاظت کے لے انھیں کنٹرول کرنے کے بجائے ان کی ذمہ داری قبول کرنی چاہئے۔

بچوں کا سیکشن

ڈیٹا سے کیا مراد ہے؟

ڈیٹا سے مراد معلومات ہیں۔ یہ معلومات آپ سے متعلق ہوتی ہیں۔ کسی کو آپ کی اجازت کے بغیر یہ حق حاصل نہیں ہے کہ ان معلومات تک رسائی حاصل کرے یا انھیں کسی پر افشا کرے۔ سوائے اس صورت کے کہ قانونی سرپرست، پولیس یا عدالتوں جیسے معتبر ادارے یا افراد تحفظ کے مقصد سے یا کسی قانونی کارروائی کے لیے اس تک رسائی حاصل کریں۔

آپ کا نام، گھر کا پتہ، فون نمبر، سکول کا نام، تصویریں اور ایسی کوئی بھی دوسری معلومات جو آپ کی شناخت کے لیے استعمال ہو سکیں، وہ آپ کے ذاتی ڈیٹا میں شمار ہوں گی۔

معلوماتی تصویر سے متعلق خیال: ذاتی ڈیٹا معلومات ہیں جنھیں آپ کی شناخت کے لیے استعمال کیا جا سکتا ہے۔ اس میں آپ کا نام، گھر کا پتہ، فون نمبر، سکول کا نام، تصویریں وغیرہ شامل ہیں۔

پرائیویسی سے کیا مراد ہے؟

پرائیویسی سے مراد ہر طرح کی مداخلت اور رکاوٹ سے آزادی ہے۔ معلومات کا اخفا ایک حق ہے تاکہ آپ اس بات کی نگرانی کر سکیں کہ آپ کے بارے میں معلومات کیسے اکٹھی اور استعمال کی جاتی ہیں۔ یہ ایک بنیادی انسانی حق ہے جو ہر کسی کو اس کے طبقے، نسل، عمر، جنس یا کسی بھی دوسرے شناختی حوالے سے قطع نظر حاصل ہوتا ہے۔

پرائیویسی انٹرنیشنل کے مطابق پرائیویسی ایک حق ہے جو ایک بنیاد کے طور پر کام کرتا ہے جس پر بہت سے دوسرے انسانی حقوق کی عمارت تعمیر کی جاتی ہے۔ اور اسی لیے اس کی بہت زیادہ اہمیت ہے۔

پرائیویسی کا حق ہمیں اس قابل بناتا ہے کہ ہم اپنی حدود خود متعین کریں اور یہ طے کریں کہ کون ان میں داخل ہو سکتا ہے۔ یہ ایک باڑ کے طور پر کام کرتا ہے جو ہمیں غیر معتبر مداخلت سے محفوظ رکھتی ہے۔ آسٹریلین انفارمیشن کمشنر کے دفتر کے مطابق پرائیویسی کے حق میں یہ حق بھی شامل ہے کہ

- مداخلت اور رکاوٹ سے آزادی حاصل ہو،
- آپ کو یہ آزادی حاصل ہو کہ جس سے چاہیں رابطہ کر سکیں، اور
- آپ کو یہ اختیار ہو کہ کون آپ سے متعلق معلومات تک رسائی حاصل کر سکتا یا انھیں استعمال کر سکتا ہے۔

پرائیویسی کا حق آپ کو یہ تحفظ دیتا ہے کہ آپ سے آپ کے بارے میں معلومات فراہم کرنے کو نہ کہا جائے۔ کسی کو یہ حق حاصل نہیں ہے کہ وہ آپ کی تصویریں، آپ کے گھر کا پتہ یا سکول کا نام کسی اور کو بتائے جب تک کہ کوئی معتبر شخص جیسے قانونی سرپرست، پولیس یا عدالت تحفظ کے مقصد سے یا کسی قانونی کارروائی کے لیے ان تک رسائی حاصل نہ کرے۔ اسی طرح کمپنیوں کو بھی یہ حق حاصل نہیں ہے کہ وہ آپ کی اجازت کے بغیر آپ سے متعلق معلومات اکٹھی کریں جیسے دوسری معلومات کے ساتھ ساتھ آپ کا پتہ اور جنس۔

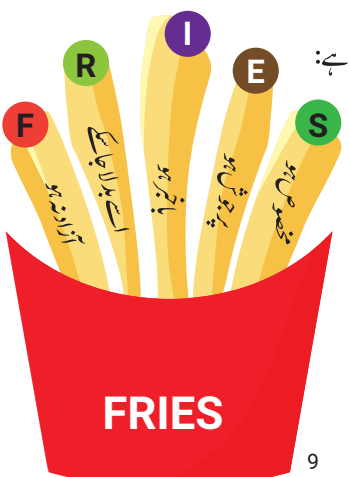
یہ جائز ہے کہ آپ پرائیویسی کا تقاضا کریں۔ آپ کچھ چھپا نہیں رہے ہیں۔ آپ کو اپنی پرائیویسی کی حفاظت کے لیے تیکنیکی ماہر ہونے کی ضرورت نہیں ہے۔

رضامندی سے کیا مراد ہے؟

تصویر اتارنے سے پہلے اجازت لیں۔

اس سے پہلے کہ کوئی آپ سے متعلق معلومات استعمال کرے، اسے آپ کی رضامندی جیسے باخبر معاہدہ حاصل کرنے کی ضرورت ہے۔ مثال کے طور پر آپ کی تصویر اتارنے سے پہلے آپ سے پوچھنا ضروری ہے۔ اسی طرح آپ سے متعلق معلومات کو استعمال کرنے سے پہلے آپ کی اجازت ضروری ہے۔ مثال کے طور پر اگر آپ فیس بک استعمال کرتے ہیں تو سوشل نیٹ ورک پلیٹ فارم کو کسی بھی مقصد کے تحت آپ سے متعلق معلومات استعمال کرنے کے لیے آپ کی اجازت لینا ضروری ہے۔ اگر آپ نابالغ ہیں تو آپ کے والدین میں سے کوئی آپ سے متعلق معلومات استعمال کرنے کی اجازت دے گا۔

رضامندی کا مفہوم یوں واضح کیا جاسکتا ہے:



بالغ اور نابالغ عمر

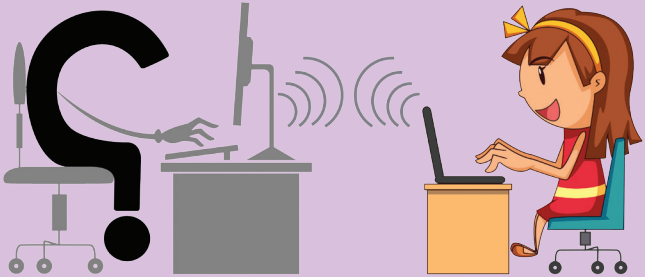
جب آپ اٹھارہ سال کے ہو جاتے ہیں تو آپ اجازت دینے کا حق حاصل کر لیتے ہیں۔ لیکن اس عمر تک آپ کی رضامندی کا دائرہ محدود رہتا ہے مثلاً اس حوالے سے فیصلہ کرنے میں آپ کے والدین یا قانونی سرپرست ایک حد تک ذمہ دار ہوتے ہیں۔

لیکن اس کا یہ مطلب نہیں ہے کہ آپ کو اپنے والدین یا قانونی سرپرستوں کے سامنے پرائیویسی کا حق حاصل نہیں ہے۔ بہت اہم ہے کہ بالغ افراد کو اس حوالے سے تعلیم دی جائے کہ بچوں اور نوجوانوں کی پرائیویسی کا احترام کتنا ضروری ہے۔

نابالغوں کے لیے سوشل میڈیا

سوشل میڈیا پر آپ کو اپنی عمر کے بارے میں غلط بیانی نہیں کرنی چاہئے۔ سوشل میڈیا کی ویب سائٹیں کسی حد تک آپ کو نابالغ ہونے کے ناطے یہ تحفظ دیتی ہیں کہ آپ کا ڈیٹا غلط انداز میں استعمال نہ کیا جائے۔ جب آپ اپنی عمر سے متعلق غلط بیانی کرتے ہیں تو آپ اس تحفظ سے محروم ہو جاتے ہیں اور آپ کے ڈیٹا کے غلط استعمال ہونے کا خدشہ بھی بڑھ جاتا ہے۔

سوشل میڈیا کی چند ویب سائٹس پر تیرا برس سے کم عمر کے بچوں کو اجازت نہیں ہوتی کہ وہ وہاں اپنے اکاونٹ بنا سکیں۔



عوامی اور ذاتی جگہوں میں فرق

آپ کا گھر آپ کی ذاتی جگہ ہے۔ کسی کو یہ حق حاصل نہیں ہے کہ وہ آپ کی ذاتی جگہ میں آپ کی اجازت کے بغیر داخل ہو۔ عوامی جگہ آپ کے گھر سے باہر واقع ہے۔ مثال کے طور پر آپ کے قریب واقع پارک میں موجود کھیل کا میدان ایک عوامی جگہ ہے۔ ایسے ہی ہسپتال اور گلیاں بھی عوامی جگہیں ہیں۔ ہم ذاتی اور عوامی جگہوں میں مختلف انداز میں برتاو کرتے ہیں۔ عوامی جگہ میں ہم زیادہ محتاط ہوتے ہیں کہ ہمیں کیسے دوسروں کے سامنے آنا اور کیسے دوسروں سے برتاو کرنا چاہئے۔ اس کے برعکس ذاتی جگہ میں آپ زیادہ آرام دہ حالت میں ہوتے ہیں۔ یہاں آپ کسی کے سامنے جواب دہ نہیں ہوتے۔ مثال کے طور پر آپ چاہیں تو بالوں میں کنگھی کیے بغیر ہی گھر میں گھومتے پھرتے رہیں۔ لیکن باہر آپ اس حالت میں نہیں جائیں گے۔

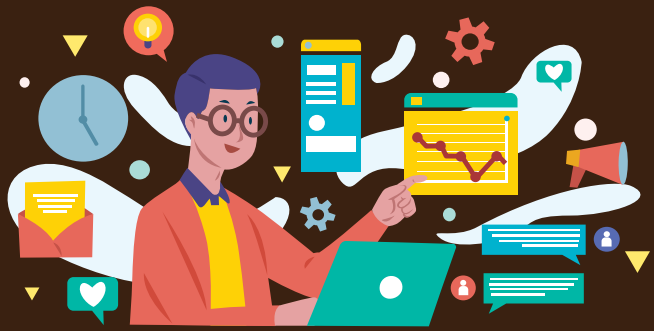
ڈیجیٹل دنیا میں بھی ذاتی اور عوامی تفریق موجود ہوتی ہے۔ آپ کا فیس بک کا پروفائل آپ کا ذاتی حوالہ ہے اور آپ کو یہ حق حاصل ہے کہ آپ فیصلہ کریں کہ اسے کس سے اور کس حد تک اسے شیئر کریں گے۔ مختصر یہ کہ آپ کو اپنے آن لائن ڈیٹا پر کسی حد تک اختیار حاصل ہوتا ہے۔ مثال کے طور پر فیس بک آپ کو اختیار دیتا ہے کہ آپ فیصلہ کریں کہ آپ کس کو اپنے سال پیدائش کے بارے میں بتانا چاہیں گے۔ جب کہ آپ کا نام اور پروفائل فوٹو فیس بک پر سب کو دکھائی دے گی جب تک آپ ان کے دکھائی دینے کو روک نہیں دیتے۔

آپ کی جیسی آف لائن شناخت ہے ویسی ہی آپ کی ایک آن لائن شناخت بھی ہے۔ یہ بہت اہم ہے کہ آپ کو ان دونوں کے درمیان موجود مماثلتوں اور اختلافات کا اندازہ

ہو کیوں کہ اس سے آپ کو اپنے ڈیٹا کو زیادہ موثر انداز میں محفوظ بنانے میں مدد ملے گی۔

ذاتی ڈیٹا کیا ہے؟

ذاتی ڈیٹا معلومات پر مشتمل ہے جو ذاتی نوعیت کی ہوتی ہیں جیسے وہ معلومات جو آپ کو شناخت کرنے کے لیے استعمال ہو سکتی ہیں۔ آپ کا نام، تصویریں، گھر کا پتہ، سکول کا نام، فون نمبر، وغیرہ۔ یہ سب آپ کے ذاتی ڈیٹا کا حصہ ہیں۔ کسی کو یہ حق حاصل نہیں ہے کہ وہ آپ سے یہ ڈیٹا مانگے جب تک کہ اسے کسی قانون نافذ کرنے والے ادارے یا عدالت کی طرف سے کوئی اختیار نہ دیا گیا ہو۔



ڈیٹا اکٹھا کرنے اور انھیں اپنے پاس رکھنے والے کون ہیں؟

ڈیجیٹل دنیا میں مختلف حوالوں سے آپ کا ڈیٹا اکٹھا کیا جاتا، اس کی چھان پھٹک کی جاتی اور اسے محفوظ کیا جاتا ہے۔ جب آپ کسی ویب سائٹ پر جاتے ہیں، تو اس بارے میں ڈیٹا حاصل کیا جاتا اور اسے اکٹھا کیا جاتا ہے کہ آپ کس ویب سائٹ پر گئے، کتنی دیر وہاں رہے اور آپ نے وہاں کیا کچھ دیکھا؟ جو کوئی اس ڈیٹا کو اکٹھا کرتا، اسے محفوظ کرتا اور پھر اس کا تجزیہ کرتا ہے، اسے ڈیٹا کلکٹر کہا جاتا ہے۔

یہ جاننا اہم ہے کہ یہ ڈیٹا کلکٹر آپ کی (یا کسی دوسرے ملک کی) حکومتیں، نجی کمپنیاں جیسے فیس بک، ٹک ٹوک یا ٹوئٹر، یا پھر کون دوسرا مقامی ادارہ ہے۔ یہ تو وہ ڈیٹا کلکٹر ہیں جو قانونی طریقوں سے ڈیٹا اکٹھا کرتے ہیں۔ لیکن بعض لوگ اس مقصد کے لیے غیر قانونی ہتھکنڈے بھی استعمال کرتے ہیں۔ جیسے ڈیٹا اکٹھا کرنے کے لیے اسے ہیک کرنا یا اسے چرا لینا۔

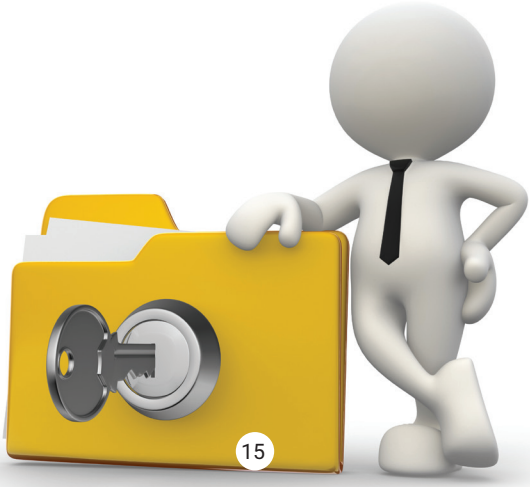
ڈیٹا اپنی تحویل میں رکھنے والے

یہ وہ لوگ یا ادارے ہیں جو یا تو آپ کے ڈیٹا کو محفوظ کرتے ہیں یا یہ ڈیٹا ان سے شیئر کیا جاتا ہے۔ ڈیٹا اپنی تحویل میں رکھنے والے ڈیٹا کلکٹر بھی ہو سکتے ہیں اور کوئی تیسرا فریق بھی جس کے ساتھ آپ کی ذاتی معلومات شیئر کی گئی ہوں۔

ڈیٹا کی حفاظت کیوں ضروری ہے؟

ٹیکنالوجی کی ترقی کا سب سے اہم نتیجہ ڈیجیٹل کے شعبے میں زیادہ سے زیادہ پیش رفت کی صورت میں سامنے آیا ہے۔ اس کا یہ مطلب بھی ہے کہ ٹیکنالوجی میں یہ امکان موجود ہے کہ وہ زیادہ سے زیادہ دخل انداز ہو سکے۔

یہ اہم بات ہے کہ آپ کو اپنے ذاتی ذاتی پر اختیار حاصل ہو۔ جیسے ٹیکنالوجی زیادہ سے زیادہ دخل انداز بنتی جا رہی ہے، اس سے یہ خطرہ پیدا ہوتا ہے کہ آپ کے ڈیٹا کو آپ کی اجازت کے بغیر کسی سے شیئر نہ کیا جائے۔ اس لیے اس بات کو یقینی بنانا بہت اہم ہے کہ آپ کا ڈیٹا محفوظ بنایا جائے۔ ڈیٹا تک رسائی کی کوششوں کی حالیہ مثالیں، جیسے نادرا اور سیف سٹی پراجیکٹ میں ہونے والی کوششیں، اس بات کو سامنے لاتی ہیں کہ کس کس انداز میں شہریوں کے ڈیٹا کو کسی سے شیئر کیا اور اس کا غلط استعمال کیا جاتا ہے۔

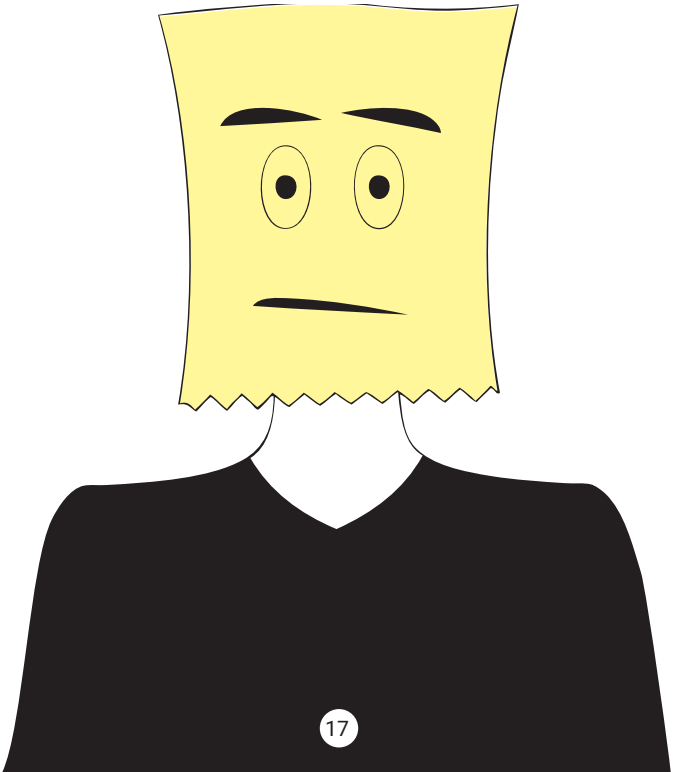


خود مختاری

جیسے آپ کو اپنے جسم پر اختیار حاصل ہے کہ یہ حق کہ کوئی اسے آپ کی مرضی کے بغیر نہ چھوئے، ایسے ہی آپ کو اپنے ڈیٹا پر بھی اختیار حاصل ہے۔ اس کا مطلب یہ ہے کہ آپ کو یہ اختیار حاصل ہے کہ آپ اپنا آن لائن ڈیٹا کتنا اور کس کس سے شیئر کریں۔ آپ اپنی پرائیویسی سیٹنگز کے ذریعے یہ اہتمام کر سکتے ہیں کہ آپ کا ڈیٹا صرف خاص افراد کے لیے ہی قابل رسائی ہو۔ مثال کے طور پر فیس بک پر آپ کو یہ اختیار حاصل ہے کہ ہر اس پوسٹ کے لیے پرائیویسی کو کنٹرول کریں جو آپ آن لائن بھیجتے ہیں۔ آپ چاہیں تو اپنی فرینڈ لسٹ میں سیٹنگز کی تبدیلی کے ساتھ انھیں یا تو سبھی سے شیئر کریں یا صرف اپنے دوستوں یا مختلف خاص دوستوں سے۔

گمنام رہنے کا حق

آپ کو یہ حق حاصل ہے کہ آپ اپنے آپ کو پس پردہ رکھیں۔ اس گمنامی کو قائم کرنے کے لیے آپ کو صارفین کو روکنا ہو گا کہ وہ آپ کے ای میل ایڈریس یا فون نمبر تک رسائی حاصل نہ کریں۔ آپ سیٹنگز ہی میں تبدیلی کے ذریعے صارفین کو روک سکتے ہیں کہ آپ کو میسیجز وغیرہ نہ بھیجیں۔



آپ کی ڈیجیٹل شناخت کے مضمرات

بعض افراد کا خیال ہے کہ سوشل میڈیا سے کسی شے کو ڈیلیٹ کر دینے سے وہ ہمیشہ کے لیے حذف ہو جاتی ہے۔ یہ بات درست نہیں ہے۔ اگر آپ پوری ویب سائٹ ہی ڈیلیٹ کر دیں تو پھر بھی آن لائن اس کی ایک کیچ موجود رہتی ہے جس میں ویب سائٹ کی دتمام انٹریز موجود ہوں گی۔ جب آپ کسی شے کو آن لائن شیئر کر لیتے ہیں تو پھر وہ آپ کی ذاتی نہیں رہتی۔

اس لیے اس بارے میں احتیاط سے کام لینے کی ضرورت ہے کہ آپ اپنے بارے میں کیا معلومات فراہم کر رہے ہیں۔ یہی وجہ ہے کہ آپ کو گوگل پر اپنے نام کو تلاش کرتے رہنا چاہئے۔ یہ نرگسیت پر مبنی حرکت نہیں ہے بلکہ ایک حفاظتی تدبیر ہے۔ آپ نہیں جان پاتے کہ آپ کے کس پرانے دوست نے، جس پر آپ بے حد اعتبار کرتے ہیں، آپ کی ذاتی معلومات مختلف آن لائن پلیٹ فارموں پر فراہم کر دی ہیں۔

حقیقت یہ ہے کہ ان دنوں بہت سے والدین اپنے بچوں کے سوشل میڈیا پروفائلز ان کے پیدا ہونے سے بھی پہلے بنا دیتے ہیں۔ وہ بچے کے فوٹو اور دیگر معلومات بھی فراہم کر دیتے ہیں۔ اس سے بچے اس حق سے محروم ہو جاتے ہیں کہ ان سے متعلق ڈیٹا فراہم کرنے سے پہلے ان کی رضامندی حاصل کی جائے۔ اس لیے یہ دیکھتے رہنا ضروری ہے کہ آپ کے والدین یا دوسرے رشتہ داروں نے آپ کے بارے میں کیا کچھ آن لائن شیئر کیا ہوا ہے۔

آپ آن لائن جو کچھ بھی کرتے ہیں، اس کا ایک نقش وہاں باقی رہ جاتا ہے جیسے یہ بات کہ آپ کون ہیں؟ یہ معلومات ویب سائٹس پر جمع ہو جاتی ہیں اور انھیں آپ کی شناخت، کھوج یا حتی کہ آپ کو تجارتی شے میں تبدیل کرنے کے لیے استعمال کیا جا سکتا ہے۔

کمپنیاں زیادہ منافع کمانے کے لیے اس ڈیٹا کو مشتہرین کو فراہم کر دیتی ہیں۔ آپ کے سبھی پسندیدہ سوشل میڈیا پلیٹ فارم جیسے فیس بک، انسٹاگرام، ٹک ٹوک ایسا ہی کرتے ہیں۔ فیس بک آپ سے جو معاہدہ کرتی ہے اس میں آپ کی طرف سے یہ اجازت شامل ہوتی ہے کہ وہ آپ سے متعلق معلومات اکٹھی کر سکتی ہے کیوں کہ اسی سے وہ پیسہ کماتی ہے۔

کیا شیئر کیا جائے اور کیا نہیں؟

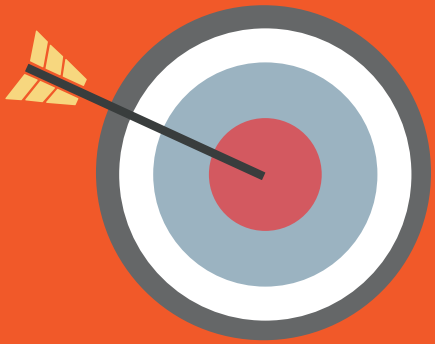
یہ طے کرنے کے لیے کہ آپ کو سوشل میڈیا پر کیا بات شیئر کرنی اور کیا شیئر نہیں کرنی چاہئے، آپ کو عوامی اور ذاتی جگہوں کے فرق پر غور کرنے کی ضرورت ہے۔ وہ بات آپ آن لائن شیئر نہ کریں جو آپ آف لائن کسی جگہ شیئر نہیں کرتے۔ مثال کے طور پر کیا آپ گلیوں میں کھڑے ہو جاتے ہیں اور وہاں اجنبی راہ گیروں کو اپنی ذاتی تصویریں بانٹتے پھرتے ہیں؟ اگر آپ ایسا نہیں کرتے تو پھر آپ کیوں ڈیجیٹل دنیا میں اپنی ذاتی تصویروں کو شیئر کرتے ہیں؟

کسی بھی معلومات کو آن لائن پوسٹ کرنے سے پہلے اپنے آپ سے پوچھیں:

- کیا کوئی یہ معلومات آپ کو نقصان پہنچانے کے لیے استعمال کر سکتا ہے؟
- کیا مجھے افسوس ہو گا اگر کوئی ان معلومات کو کسی اور سے شیئر کرے؟
- کیا مجھے آف لائن یہ معلومات کسی کو دینا پسند ہو گا؟

ان سوالات پر غور کرنا بہت اہم ہے جو اس فیصلے کو ممکن بنانے کے لیے کیے جائیں گے کہ آپ کو اپنے بارے میں معلومات آن لائن کسی سے شیئر کرنی چاہئے یا نہیں۔

عملی مثال



کیسے اپنے ڈیٹا کی حفاظت کی جائے؟

آپ کے ڈیٹا کو کسی سے شیئر کرنے کے لیے ضروری نہیں ہے کہ اسے چرایا جائے یا فریب سے حاصل کیا جائے۔ اکثر اوقات ہم اپنے ڈیٹا کے غلط استعمال کو درپیش خطرات سے نمٹنے میں سستی یا غفلت کا مظاہرہ کرتے ہیں۔

اپنی ڈیوائس کو محفوظ بنایئے

اگر آپ کے پاس کوئی ڈیوائس ہے جیسے کمپیوٹر، موبائل فون یا ٹیبلٹ تو آپ اسے حفاظتی کوڈ سے محفوظ بنائیں۔ ایک پاس ورڈ یا پاس کوڈ اس بات کو یقینی بنائے گا کہ آپ کی ڈیوائس تب محفوظ ہو گی جب اسے یونہی کہیں کھلا چھوڑ دیا جائے یا پھر یہ گم یا چوری ہو جائے۔

وائرس اور مال ویئر سے تحفظ

مال ویئر نقصان دہ سافٹ ویئر' کا مخفف ہے۔ ایسے سافٹ ویئر آپ کے کمپیوٹر سسٹم کو نقصان پہنچانے کا باعث بن سکتے ہیں۔ یاد رکھئے کہ تمام وائرس مال ویئر ہوتے ہیں لیکن تمام مال ویئر ضروری نہیں ہیں کہ وہ وائرس بھی ہوں۔ دنیا بھر میں پیشہ ور جرائم پیشہ افراد اور ڈیٹا چرانے والے مختلف قسموں کے مال ویئر تیار کرتے ہیں تاکہ آپ کے کمپیوٹر کو ہدف بنائیں اور مثال کے طور پر آپ کے بنک سے متعلق معلومات چرا کر آپ کی جاسوسی کر سکیں۔ اپنی ڈیوائس کی حفاظت کے لیے آپ کے پاس انٹی وائرس سافٹ ویئر اور انٹی مال ویئر سافٹ ویئر ہونا چاہیئے۔ آپ کے پاس آواسٹ، اے وی جی، ایویرا، کیسپر سکی اور نورٹن جیسے انٹی وائرس سافٹ ویئر وائرسوں کے خلاف اور مال ویئر بائیٹس، لاواسافٹ اور سپائی بوٹ جیسے سافٹ ویئر مال ویئر کے خلاف ہونے چاہئیں۔

خبردار، ہم کسی کی یو ایس بی ڈرائیو استعمال کرنے یا کسی کو اپنی ڈرائیو استعمال کرنے کی اجازت دینے کا مشورہ نہیں دیتے۔ بعض اوقات کوئی جان بوجھ کر بھی آپ کی یو ایس بی ڈرائیو میں مال ویئر منتقل کر دیتا ہے تاکہ جس بھی کمپیوٹر میں یہ استعمال کی جائے، وہ اسے متاثر کر دے۔

McAfee

Norton by Symantec | LifeLock

Malwarebytes

avast

کام کی بات: جب بھی یو ایس بی استعمال کریں، اسے انٹی وائرس اور انٹی مال ویئر سافٹ ویئر کے ذریعے ہی چلائیں۔

بیک اپ

کیا کبھی ایسا ہوا ہے کہ آپ نے اپنے کمپیوٹر میں کوئی پریزنٹیشن محفوظ کی ہو، آپ کا کمپیوٹر خراب ہو گیا ہو؟ ڈیٹا کا گم ہو جانا ایک مایوس کن بات ہے۔ بعض اوقات یہ پھر سے حاصل کیا جا سکتا ہے۔ اس لیے ہماری تجویز یہ ہے کہ آپ اپنے اہم ڈیٹا کو بیک اپ کے ذریعے محفوظ بنائیں جیسے جیسے اسے ہارڈ ڈرائیو میں کاپی کر کے۔ چوں کہ کلاؤڈ اسے ہارڈ ڈرائیو میں کاپی کر کے۔ چوں کہ کلاؤڈ کے ذریعے ڈیٹا کا ذخیرہ ایک آسان طریقہ ہے اور اس کے لیے کسی ڈیوائس کی بھی ضرورت نہیں ہے، آپ اس میں جو ڈیٹا منتقل کرتے ہیں، وہ آن لائن باقی رہتا ہے۔ اس ڈیٹا کو بھی چوری کیا جا سکتا یا فریب سے ہتھیایا جا سکتا ہے۔ لیکن زیادہ اہم بات یہ ہے کہ جو شے آن لائن منتقل ہو جاتی ہے، وہ ہمیشہ کے لیے ایک نشان چھوڑ دیتی ہے۔ اس لیے بہتر یہ ہے کہ اہم ذاتی ڈیٹا کو محفوظ کرنے کے لیے ہارڈ ڈرائیو یا یو ایس بی استعمال کی جائے۔ آپ کو ہمیشہ یاد رکھنا چاہئے کہ آپ نے ہارڈ ڈرائیو کہاں رکھی تھی، تاکہ ضرورت کے وقت آپ کو اس کی تلاش میں مشکل نہ ہو۔

پاس ورڈ مضبوط بنائیں

آپ نہیں چاہتے کہ آپ کا پاس ورڈ کمزور ہو تاکہ اسے آسانی سے بوجھ لیا جائے۔ یہ کافی نہیں ہے کہ پاس ورڈ طویل ہو۔ اس کے بجائے آپ کو مضبوط خفیہ جملوں کے بارے میں سوچنا چاہئے جو چھ یا آٹھ خفیہ الفاظ سے زیادہ لمبے ہوں اور اگر انھیں چالاکی سے بنایا جائے تو انھیں بوجھنا مشکل ہو۔

آپ کا خفیہ جملہ ایسا ہونا چاہئے

- اٹھارہ سے تیس حروف پر مشتمل ہو
- ایسے الفاظ پر مشتمل ہو جو لغات یا معروف اقوال میں نہ ڈھونڈے جا سکیں
- ایک لفظ سے زیادہ لمبا ہو
- بڑے اور چھوٹے دونوں طرح کے حروف، اعداد اور اشارات پر مشتمل ہو

آپ کے خفیہ جملے ایسے نہیں ہونے چاہئیں

- آپ کی ذاتی اور آسانی سے بوجھ لی جانے والی معلومات پر مبنی نہ ہوں جیسے آپ کی تاریخ پیدائش، آپ کا گھریلو نام، وغیرہ
- آپ کی ذاتی پسند و ناپسند یا مشاغل پر مبنی نہ ہوں
- آپ کی ڈیوائس میں کسی دستاویز یا کسی کاغذ کے ٹکڑے پر اسے نہ لکھا گیا ہو۔

کام کی بات: بہترین دوست اور پیار کرنے والے آپ سے پاس ورڈ کا تقاضا نہیں کرتے۔ اس کے بجائے وہ آپ کی پرائیویسی کی قدر کرتے ہیں۔ کسی سے بھی اپنا پاس ورڈ شیئر مت کریں جب تک کہ ایسا کرنا آپ کے اور دوسروں کے تحفظ کے لیے ناگزیر نہ ہو جائے۔

کام کی بات: ہر پرانی شے سونا نہیں ہوتی۔ یہ غیر محفوظ بات ہے۔ اپنے پاس ورڈ کو وقتاً فوقتاً بدلتے رہیں۔

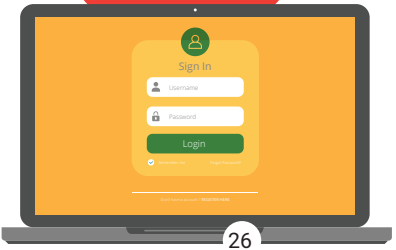
اگر آپ کے لیے بہت سے پاس ورڈ یاد رکھنا مشکل ہوں تو 'کیپ پاس' اس کا ایک حل ہے۔ یہ بالکل مفت دستیاب ہوتا ہے۔ یہ ایک فائدہ مند شے ہے جو آپ کے لیے مضبوط پاس ورڈ تیار اور محفوظ کرتا ہے۔ آپ کو صرف ایک ماسٹر پاس ورڈ یاد رکھنے کی ضرورت ہوتی ہے جسے ایک مضبوط اور ناقابل دریافت خفیہ جملہ ہونا چاہئے۔ اس بات کا یقین کر لیں کہ آپ اپنا کیپ پاس ڈیٹا بیس کسی بیرونی جگہ محفوظ کریں کیوں کہ اگر آپ اسے اپنے کمپیوٹر میں محفوظ کریں گے تو چور اس تک رسائی پا لیں گے۔

دوہری تصدیق

دوہری تصدیق کا طریقہ آپ کی سوچ سے بھی زیادہ آسان ہے۔ آپ اپنے فون اور موبائل فون کے نمبر کو اپنے آن لائن اکاونٹ سے جوڑ کر اس پر حفاظت کی ایک اضافی تہہ جماتے ہیں۔ اس طریقے سے جب آپ لاگ ان ہوتے ہیں تو آپ کو ایک کوڈ درج یا منتخب کرنا پڑتا ہے جو پھر ایک ٹیکسٹ میسیج، ایک خودکار ٹیلی فون کال یا گوگل آتھینٹی کیٹر جیسی کسی ایپ کے ذریعے آپ کو بھیجا جاتا ہے۔

آتھینٹی کیٹر ایپس پاکستان جیسے ملکوں کے صارفین کے لیے مثالی ہیں جہاں موبائل فون کے سگنلز کو عید یا ایسے ہی دیگر مواقع پر روک دیا جاتا ہے۔ یہ ایپس ہر بار کھولے جانے پر آپ کو ایک کوڈ فراہم کرتی ہیں۔ یہ اس صورت میں بھی فائدہ مند ہیں کہ جب آپ بیرون ملک سفر پر ہوں اور اپنی دوہری تصدیق کی ایپ بند کرنا بھول گئے ہوں۔

دوہری تصدیق کی ایپ استعمال کرنے کا مطلب یہ نہیں ہے کہ آپ کمزور پاس ورڈز رکھیں۔



براوزنگ کا تحفظ

انٹرنیٹ ایکسپلورر، موزیلا فائر فوکس اور گوگل کروم انٹرنیٹ ویب براوزر کی مثالیں ہیں۔ اگر آپ کی ڈیوائس میں انٹی وائرس اور انٹی مال ویئر سافٹ ویئر کام کر رہے ہیں، تب بھی آپ کا براوزر خطرے سے خالی نہیں ہے۔ اس لیے آپ کو اپنے براوزر کے تحفظ کے لیے چند مزید اقدامات کرنے کی ضرورت ہے۔

ا۔ اپنے اکاونٹس کو سائن ان حالت میں مت چھوڑیں۔ چاہے آپ اپنی ڈیوائس کو استعمال کرنے والے واحد صارف ہوں۔ آپ کی ڈیوائس گم ہو سکتی ہے، یا اسے چوری کیا جا سکتا ہے یا اسے ہیک کیا جا سکتا ہے۔

ب۔ کوئی ذاتی ونڈو (فائر فوکس) استعمال کریں یا پھر اپنی شناخت ظاہر کیے بغیر کوئی پروگرام استعمال کریں جیسے گوگل کروم۔ تاکہ آپ کے براوزر میں ان ویب سائٹس کا، جن کو آپ نے ملاحظہ کیا اور ان پاس ورڈز کا جو آپ نے وہاں لکھے، ریکارڈ باقی نہ رہے۔

ج۔ اپنی براوزنگ کی تاریخ کبھی محفوظ نہ کریں۔ اسے آپ اپنے براوزر کی سیٹنگ میں جا کر تبدیل کر سکتے ہیں۔

د۔ کوکیز اور انٹرنیٹ کی عارضی فائلوں کو باقاعدگی سے ڈیلیٹ کرتے رہیں۔

ر۔ براؤزر کی Do not track کو منتخب کریں تاکہ ویب سائٹس آپ کو کھوج نہ سکیں۔ سیٹنگز میں

س۔ کسی ایسی ویب سائٹ میں اپنا پاس ورڈ نہ لکھیں جو کسی ادارے کی ای میل یا سوشل میڈیا ویب سائٹ نہ ہو۔

ش۔ کبھی کسی یونہی سامنے آنے والی ویب سائٹس کو اپنے بارے میں حساس معلومات نہ دیں جیسے آپ کے کریڈٹ کارڈ سے متعلق معلومات۔

براؤزر ایڈ اونز

آپ ایڈ آن یا ایکسٹینشنز کے ذریعے تحفظ کے انتظام کو مزید مضبوط بنا سکتے ہیں۔ یہ کوکیز، ٹریکرز اور پوپ اپ ایڈز کو روک کر آپ کی پرائیویسی اور تحفظ کو یقینی بنا سکتے ہیں۔

ا۔ Https Everywhere:

یہ ایڈ آن اس بات کو یقینی بناتا ہے کہ آپ ہر جگہ بناتا ہے کہ آپ ایچ ٹی ٹی پی کے ذریعے محفوظ انداز میں کسی ویب سائٹ سے رابطے میں رہیں جو آپ کی معلومات کو محفوظ رکھے گا نہ کہ کسی غیر محفوظ ایڈ آن کے ذریعے صرف وہیں تحفظ دے گا جہاں ممکن ہو گا۔

ب۔ پرائیویسی بیجر:

یہ ایڈ آن اس بات کو یقینی بناتا ہے کہ کوئی دوسری ویب سائٹ آپ کو کھوج نہیں سکے گی۔

ج۔ نوسکرپٹ:

یہ ایک چھوٹا سا پروگرام ہے جو بعض ویب سائٹس آپ کے براؤزر میں چلاتی ہیں۔ بعض اوقات یہ سکرپٹس غیر محفوظ ہوتے ہیں اور اس لیے آپ کو 'نوسکرپٹ' کی ضرورت ہوتی ہے۔

اپنی سوشل میڈیا کو کیسے محفوظ اور گمنام رکھا جا سکتا ہے

سوشل میڈیا تب ایک دردسر بن سکتا ہے جب آپ کے تحفظ کے انتظامات کمزور ہوں۔ اس بارے میں خاص طور پر آپ کو محتاط ہونے کی ضرورت ہے خاص کر سوشل میڈیا کے پلیٹ فارمز پر اپنی سیکیورٹی اور پرائیویسی کی سیٹنگز کو مستقل طور پر تبدیل کرتے رہیں۔ اس کا مطلب یہ ہے کہ جو معلومات پہلے ذاتی حیثیت میں تھیں یا صرف خاص صارفین کے لیے ہی قابل رسائی تھیں، وہ اب اچانک آپ کے سبھی دوستوں یا عام لوگوں کے لیے قابل ملاحظہ ہو چکی ہیں۔

آن لائن سیکیورٹی کے لیے بنیادی باتیں

ا۔ کوئی پوسٹ تیار کرتے ہوئے احتیاط کیجئے کہ آپ کیا معلومات وہاں دے رہے ہیں۔ اگر آپ گلیوں میں کھڑے ہو کر اپنی ذاتی تصویریں وہاں سے گزرتے راہ گیروں کو نہیں دینا چاہیں گے تو پھر کیوں کر آپ انھیں آن لائن دوسروں کو دکھانے پر تیار ہوں گے۔ صرف وہی معلومات آن لائن دوسروں سے شیئر کریں جو آپ کی شناخت کے لیے ضروری ہیں۔

ب۔ اپنی سیکیورٹی اور پرائیویسی سے متعلق سیٹنگز کو اپ ڈیٹ کرنے کے لیے انھیں بدلتے رہیں۔ اس سے یہ بھی یقینی ہو جاتا ہے کہ سوشل میڈیا پلیٹ فارمز پر ہونے والی تبدیلیاں آپ کی سیکیورٹی اور پرائیویسی پر اثر انداز نہیں ہوتیں۔

ج۔ آپ پرائیویسی سے متعلق اپنی سیٹنگز تبدیل کر کے اپنی گمنامی کو برقرار رکھ سکتے ہیں تاکہ صارفین کو آپ کے ای میل کے پتے یا فون نمبر کے ذریعے آپ تک پہنچنے کی راہ نہ ملے۔ آپ پرائیویسی کی سیٹنگز میں تبدیلی کر کے بھی صارفین کو روک سکتے ہیں کہ وہ آپ کو میسیجز نہ بھیجیں۔

د۔ فیس بک اور گوگل آپ کو اس بات کی اجازت دیتے ہیں کہ کہاں آپ 'لاگ ان' ہیں اور کہاں آپ 'لاگ آن' ہیں۔ ان معلومات کا باقاعدگی سے جائزہ لیں تاکہ آپ کو یقین ہو سکے کہ آپ نے کہیں کسی ویب سائٹ پر کوئی سیشن یونہی تو نہیں چھوڑ دیا ہے یا یہ کہ آپ کے اکاؤنٹ میں کوئی دخل اندازی تو نہیں ہوئی ہے۔

ر۔ اس بات کو یقینی بنائیں کہ سوشل میڈیا کی ویب سائٹس خاص کر آپ کو اشتہارات نہ بھیجیں یا آپ کو آن لائن نہ کھوج لیں۔ اپنی فیس بک میں اشتہارات سے متعلق ترجیحات کا جائزہ لیں۔ آپ کو یہ جان کر حیرت ہو گی کہ وہاں 'اشتہارات سے متعلق ترجیحات' کو شناخت کرنے کے لیے آپ سے متعلق بنیادی الفاظ کی بڑی تعداد موجود ہے۔

س۔ کبھی سوشل میڈیا ویب سائٹس کو اپنی جگہ کا پتہ نہ دیں۔ اس بات کو یقینی بنائیں کہ اس سے متعلق آپشن کو سیٹنگز میں جا کر ڈس ایبل کر دیں۔

ش۔ چیک ان' کے آپشن کے ذریعے کبھی سوشل میڈیا پر یہ نہ بتائیں کہ 'آپ کہاں ہیں۔

ص۔ اپنی ٹیگ سے متعلق سیٹنگز کی جانچ کریں اور انھیں بدلتے رہیں تاکہ یہ بات یقینی ہو سکے کہ آپ کو غیر متعلقہ تصویریں اور اپ ڈیٹس ٹیگ نہ کیے جائیں۔

کام کی بات: جو کچھ بھی آپ آن لائن کرتے ہیں، وہ وہاں باقی رہتا ہے۔ اگر ویب سائٹ ڈیلیٹ بھی ہو جائے تو وہاں ایک کا ایک کیچ باقی رہے گا جس میں آپ کی ویب سائٹ پر جانے کی معلومات موجود ہوں گی۔ اس لیے سوشل میڈیا کو اس خیال کے ساتھ استعمال کریں کہ ڈیجیٹل دنیا میں کوئی شے ذاتی نہیں رہتی۔

وی پی این

وی پی این سے مراد ورچوئل پرائیویٹ نیٹ ورک ہے۔ آپ وی پی این کو اس لیے استعمال کرتے ہیں تاکہ دوسرے ملکوں میں سرور پر آپ کے براؤزر کے ذریعے کسی کو آپ کے پتے کا علم نہیں ہو سکے گا۔

ہاٹ سپاٹ بھی وی پی این کی ایک سروس ہے جسے آپ اپنے کمپیوٹر پر مفت انسٹال کر سکتے ہیں۔ پھر بھی یہ آپ کے کمپیوٹر کو ظاہر کر سکتی ہے۔ اس میں آپ کے استعمال میں آنے والے لاگز بھی موجود رہتے ہیں۔

بہترین طریقہ یہ ہے کہ ادائیگی کے ذریعے زیادہ محفوظ وی پی این تلاش کیے جائیں جیسے ڈس کنکٹ یا ٹنل بیئر۔ دوسرا طریقہ یہ ہے کہ براؤزر میں وی پی این ایڈ آن استعمال کیا جائے جیسے زین میٹ۔

VPN

ZenMate

بہتر ہے کہ آپ اپنی ڈیوائس کو یہ اجازت نہ دیں کہ وہ آپ کے پتے کی شناخت کرے۔ جب ہم اپنے فون یا دوسری ڈیوائسز میں آن لائن نقشہ جات سے رہنمائی حاصل کرتے ہوئے پتہ ڈھونڈنے کی سروسز استعمال کرتے ہیں تو ہم اکثر یہ بھول جاتے ہیں کہ ایسا کرتے ہوئے ہم اس ایپلیکیشن کو یہ اجازت دے رہے ہوتے ہیں کہ وہ کسی بھی وقت آپ کے پتے کو کھوج لے سوائے اس وقت کہ جب ہم اسے بند کر دیں۔ اگر آپ پتہ تلاش کرنے کی سروس کو ڈس ایبل نہیں کرتے تو آپ کی ڈیوائسز آسانی سے تلاش کر سکتی ہیں کہ آپ واقعتاً کہاں موجود ہیں۔

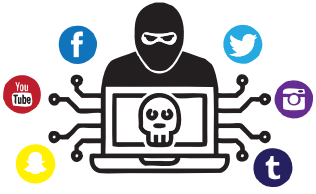
اشارہ: اگر آپ سمت کی جانچ کرنا چاہتے ہیں یا نقشہ استعمال کرنے کی ضرورت ہے تو، اپنی محل وقوع کی خدمت اسی وقت رکھو جب آپ نقشہ استعمال کر رہے ہو۔ اس بات کو یقینی بنائیں کہ آپ دوسرے تمام اوقات میں اسے بند کرتے رہتے ہیں۔

سائبر ہراسانی کو سمجھئے

آپ کیا کریں گے اگر کوئی فرد جب بھی چاہے شور مچاتا ہوا آپ کے دروازے پر دستک دینے لگے۔ یا آپ کو برا بھلا کہے یا آپ کو بدنام کرے؟ یا یہ کہ کوئی آپ کے گھر کے باہر کھڑا دن رات آپ کو گالیاں دیتا رہے؟ آپ پولیس یا کسی کو مدد کے لیے بلائیں گے۔ یہی کریں گے نا۔

عام طور پر ہراسانی کو تب سنجیدگی سے لیا جاتا ہے جب کوئی فزیکل طور پر ایسا کرے۔ لیکن لوگ اس بارے میں نہیں جانتے کہ اگر ایسا ہی سائبر کی دنیا میں ہو تو کیا کریں۔ ہم لوگوں کے حق کا تب تو احترام کرتے ہیں یعنی جب معاملہ فزیکل ہو جیسے گھر میں یا دفتر میں۔ لیکن جب کسی کو ڈیجیٹل دنیا میں ہراسانی یا دھونس دھمکی کا سامنا ہو تو زیادہ تر لوگ متاثرہ شخص ہی کو مورد الزام ٹھہراتے ہیں۔

یہ یاد رکھنا بہت اہم ہے کہ کسی فرد کی آن لائن شخصیت بھی اتنی ہی قابل قدر ہے جتنی اس کی جسمانی شخصیت۔ جیسی عوامی جگہ ہوتی ہے ایسے ہی انٹرنیٹ بھی ہر کسی کی ملکیت ہے۔ حقیقی عوامی جگہوں میں کسی کو یہ حق حاصل نہیں ہوتا کہ وہ آپ کی پرائیویسی میں داخل ہو کر آپ کو پریشان کرے یا آپ کو ہراساں کرے یا آپ کو ڈرائے دھمکائے۔ یہ اصول آپ کی آن لائن ذاتی جگہ پر بھی ویسے ہی لاگو ہوتے ہیں۔ اس لیے اس کی کوئی وجہ نہیں ہے کہ آپ سائبر دنیا میں ہراساں کیے جانے کو نظر انداز کریں۔



بعض اوقات ہم لوگوں کو روک دیتے ہیں کہ وہ ہمیں برا بھلا نہ کہیں۔ لیکن آن لائن بدسلوکی کرنے والے چند لوگ جنھیں عام طور پر ٹرالز یعنی ناپسندیدہ افراد کہا جاتا ہے، آپ کے بلاک کیے جانے پر نئے اکاؤنٹس کھول لیتے ہیں۔ کیا آپ نے سوچا کہ وہ ایسا کیوں کرتے ہیں؟ ہمارے خیال میں اس لیے کہ وہ آپ کو خاموش کر دینا چاہتے ہیں۔ جب کہ یہ درست نہیں ہے کہ آپ کو یوں خاموش کرنے کی کوشش کی جائے۔

یاد رکھئے:

- اگر کوئی آپ سے آن لائن بدسلوکی کر رہا ہے یا آپ کے بارے میں ایسی باتیں کر رہا ہے جو آپ کو پریشان کریں تو ضروری نہیں ہے کہ ہمیشہ یہ آپ ہی کی غلطی کی وجہ سے ہو۔
- اگر آپ اپنی رائے کا اظہار کر رہے ہیں جسے دوسرے ناپسند کرتے ہیں تو اس کا مطلب یہ نہیں ہے کہ آپ کو برا بھلا کہا یا ڈرایا دھمکایا جائے۔
- آپ کبھی ایسا نہیں چاہیں گے۔

یاد رکھئے:

- آپ آن لائن اس لیے موجود ہیں کیوں کہ یہ آپ کا حق ہے کہ آپ انٹرنیٹ استعمال کریں۔
- اگر کوئی آپ کو یہ کہتا ہے کہ آپ انٹرنیٹ استعمال نہ کریں تو وہ آپ کو آپ کے حق سے محروم کر دینا چاہتا ہے۔
- آپ فیصلہ کرتے ہیں کہ آپ آن لائن بدسلوکی کرنے والے کسی فرد کو بلاک کریں اور کس کا سامنا کریں۔ چند لوگ بدسلوکی کرنے والوں سے نمٹنے کی کوشش کرتے ہیں اور ایسا وہ کر پاتے ہیں۔
- اگر آپ سائبر دنیا میں ڈرائے جانے کے بعد اپنا اکاؤنٹ ڈی ایکٹی ویٹ کر لیتے ہیں تو یہ آپ کو دھمکانے والے کی کامیابی ہے۔ یعنی آپ نے اپنی جگہ اس کے لیے چھوڑ دی۔

پرائیویسی کی خلاف ورزی پر کیا کیا جائے؟

اگر کوئی آپ کے کمپیوٹر یا موبائل فون تک رسائی حاصل کر لیتا ہے اور آپ کا ڈیٹا چوری کر لیتا یا اسے افشا کرتا ہے تو اس کا مطلب یہ ہے کہ پرائیویسی کی خلاف ورزی کی گئی ہے۔ پرائیویسی کی خلاف ورزی تب ہوتی ہے جب کوئی آپ کی اجازت کے بغیر آپ سے متعلق معلومات تک رسائی حاصل کر لیتا ہے۔

پرائیویسی کی خلاف ورزی کے بعد آپ کو یہ چند اقدامات کرنے چاہئیں۔

ا۔ اپنے پاس ورڈ کو پھر سے منتخب کریں۔ یقین کر لیں کہ مختلف ویب سائٹس کے لیے آپ کے پاس ورڈز مختلف ہیں۔

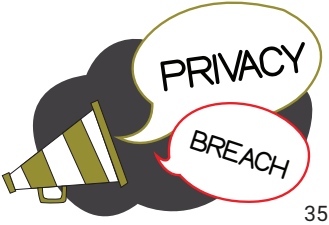
ب۔ دوہری تصدیق کا بندوبست کریں۔

ج۔ اپنے بنک سے متعلق معاملات پر نگاہ رکھیں اور جب آپ کو لگے کہ کچھ مشکوک سرگرمی ہو رہی ہے تو اپنا پن کوڈ تبدیل کر لیں۔

د۔ اپنے بنک سے متعلق سرگرمیوں کو تب روک لیں، اگر آپ دیکھیں کہ آپ کے اکاونٹ میں کچھ مشکوک سرگرمی جاری ہے۔

ر۔ ایک مضبوط پاس کوڈ بنا کر، یا اپنی ڈیوائس کو بند کرنے کے لیے انگلیوں کے نشان یا چہرے کی شناخت جیسے انتظامات کے ذریعے اپنے سمارٹ فون کو محفوظ بنائیں۔

س۔ اچھے معیار کے انٹی وائرس اور انٹی مال ویئر سافٹ ویئر استعمال کریں۔



آپ کا ڈیٹا کیسے آپ کے خلاف استعمال ہو سکتا ہے؟

چوری شدہ ڈیٹا کسی 'ڈارک ویب' پر پہنچ جاتا ہے جو انٹرنیٹ کے اس حصے میں کام کر رہی ہوتی ہے جس تک زیادہ تر لوگوں کی رسائی نہیں ہوتی۔ سائبر جرائم پیشہ افراد دیگر کارروائیوں کے ساتھ ساتھ اس ویب سائٹ کو آپ کے ذاتی ڈیٹا کو خریدنے یا بیچنے کے لیے بھی استعمال کرتے ہیں۔ جب آپ ایک ہی پاس ورڈ کو مختلف ویب سائٹس کے لیے بار بار استعمال کرتے ہیں تو آپ ہیکروں اور دھوکے بازوں کے لیے چوری کو آسان بنا دیتے ہیں۔ اس سے سائبر جرائم پیشہ افراد کو سہولت مل جاتی ہے کہ وہ کسی ایک ویب سائٹ سے آپ کا لاگن چرائیں اور اسے کسی دوسری ویب سائٹ پر آپ کے اکاؤنٹ کو ہیک کرنے کے لیے استعمال کریں۔ خاص طور پر اگر آپ کے بنک سے متعلق معلومات چوری ہو جائیں تو آپ کو مالی نقصانات کا بھی سامنا ہو جاتا ہے۔ ایسے ذاتی ڈیٹا، جو آپ کی شناخت سے متعلق ہو، کی چوری کا مطلب یہ ہے کہ جنھیں آپ کے ڈیٹا تک رسائی حاصل ہے وہ بہروپ بدل کر آپ سے رابطہ کر سکتے ہیں۔ اس سے آپ کو فزیکل خطرے کا سامنا ہو سکتا ہے۔

یہ دیکھنے کے لیے کہ کیا آپ کا ای میل کا پتہ ڈیٹا کی خلاف ورزی کا شکار تو نہیں ہو گیا ہے، یہ سائٹ ملاحظہ کیجیے

https://haveibeenpwned.com/

والدین

بچوں کے لیے انٹرنیٹ ایک پر لطف جگہ ہو سکتی ہے۔ لیکن اس کے چند نقصانات بھی ہیں۔ اس لیے بہت اہم ہے کہ والدین اپنے بچوں سے ان کی فزیکل حفاظت ہی کی طرح ان کی آن لائن حفاظت کے لیے بھی مکالمہ کریں۔ بلا تکلف مکالمہ آپ کے بچوں کو آن لائن ایک محفوظ اور مثبت زندگی گزارنے میں معاون ثابت ہو سکتا ہے۔ آپ کو اپنے بچے کی حوصلہ افزائی کرنی چاہئے کہ وہ آپ سے اپنی آن لائن خوش گوار سرگرمیوں کے بارے میں بات چیت کرے۔

کام کی بات: اگر آپ کا بچہ آپ کے سامنے اپنا کوئی مسئلہ پیش کرتا ہے تو خود کو پر سکون رکھتے ہوئے اسے سنیں اور محتاط رہیں اور غصے میں مت آئیں۔

ہم ان والدین کی حوصلہ شکنی کرتے ہیں جو اپنے بچوں اور ان کی آن لائن سرگرمیوں سے متعلق سخت رویہ اپناتے ہیں۔ والدین کی حیثیت میں آپ کا کردار ایسے معاون شخص کا ہونا چاہئے جو اپنے بچے کو اس قابل بنائے کہ وہ اپنی پرائیویسی کا زیادہ بہتر انداز میں تحفظ کر سکے۔ پاکستان میں بہت سے والدین اپنے بچوں کے حوالے سے ایک تحکمانہ اور دبانے والے کا رویہ اپنانے کو ترجیح دیتے ہیں۔ وہ ایسا زیادہ تر ان کی حفاظت کے خیال ہی سے کرتے ہیں، لیکن ایسا رویہ غیر موثر ثابت ہوتا ہے کیوں کہ اس طرح وہ اپنے بچوں سے اعتماد کا تعلق قائم کرنے میں ناکام ہو جاتے ہیں۔

اعتماد کے تعلق کے بغیر بچوں کو درپیش خطرات کہیں سنگین ہو سکتے ہیں جیسے یہی کہ وہ رازداری کا رویہ اپنا لیتے ہیں اور چوری چھپے مختلف سرگرمیوں میں مصروف رہنے لگتے

ہیں۔ ایک اصول کے طور پر آن لائن ویب سائٹس کی ممانعت کرنا ایک بہتر طریقہ نہیں ہے کیوں کہ ڈیجیٹل ویب سائٹس کی بیک وقت ہر جگہ موجود ہونے کی خصوصیت کے باعث یہ طریقہ مسلسل ناممکن ہو رہا ہے۔ مزید یہ کہ انٹرنیٹ تک رسائی سے انکار اپنے بچے کے لیے بہت سے مواقع سے انکار کے برابر ہے۔ انٹرنیٹ کی دنیا سے متعلق بچے کو ایسے ہی باخبر بنایئے جیسے آپ حقیقی دنیا کے بارے میں اسے بتاتے ہیں کیوں کہ آن لائن بھی اسے ویسے ہی خطرات لاحق ہوتے ہیں جیسے حقیقی دنیا میں۔ انٹرنیٹ میں موجود خطرات کے بیان کے لیے حقیقی دنیا سے مثالیں لیں۔ البتہ آخری فیصلے کا اختیار بچے ہی کے پاس رہنے دیں۔

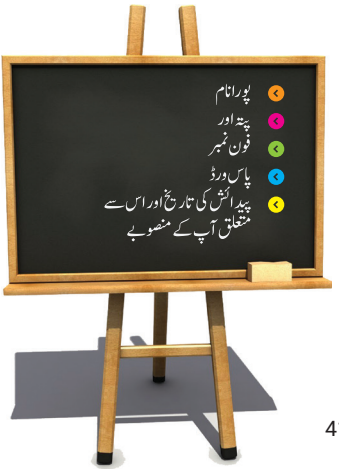
آپ کو خاص طور پر اس بارے میں اپنے بچے سے بات کرنی چاہئے کہ شکاری کیسے بچوں یا ٹین ایج لڑکیوں لڑکوں کا مختلف بہروپ میں سوشل میڈیا کی ویب سائٹس پر شکار کرتے ہیں۔ ایسا کرنے سے وہ بچے کو مائل کرتے ہیں کہ وہ اپنی ذاتی معلومات انھیں دیں۔

ایک فیصلہ کن حتمی رویہ اپنائے بغیر اپنے بچے کو آن لائن چیلنجز کے بارے میں آگاہی دیں۔ ان کا شکریہ ادا کریں کہ انھوں نے آپ کو اپنے مسائل سے آگاہ کیا۔ ان پر الزام تھوپنے کے بجائے مسئلے کو حل کرنے کے رویے پر توجہ مرکوز کریں۔ اس سے نہ صرف آپ کا اپنے بچے سے پر اعتماد رشتہ مضبوط ہو گا بلکہ اس سے وہ زیادہ سے زیادہ اس قابل ہو سکیں گے کہ آپ کی مثال کی پیروی کرتے ہوئے مسائل کو حل کرنے کے طریقوں کی طرف مائل ہوں۔

یہاں چند نکات بیان کیے جا رہے ہیں جو آپ اپنے بچوں کو آن لائن درپیش خطرات کے بارے میں آگاہ کرتے ہوئے دھیان میں رکھیں۔

- بہت شروع کی عمر ہی میں آپ اپنے بچوں کو آگاہ کریں کہ آن لائن ان کا رویہ کیا ہو اور احتیاطی تدابیر کیا ہونی چاہئیں۔
- ان کی حوصلہ افزائی کریں کہ جب وہ پریشان ہوں تو آپ سے بات کریں اور جب بھی وہ کسی غیر معمولی معاملے کو لے کر آپ کے پاس آئیں، ان کی باتیں سنجیدگی سے سنیں۔
- بچوں کو آن لائن احتیاطوں کے بارے میں بتائیں جیسے اجنبیوں سے بات کرنا وغیرہ۔
- بچوں کو مضبوط پاس ورڈز بنانے اور انھیں کبھی کسی کو نہ بتانے کی اہمیت کے بارے میں بتائیں۔
- بچوں کو وائرسوں کے بارے میں آگاہ کریں اور یہ بھی کہ اپنی ڈیوائسز کو اس حوالے سے سکین کرنا کیوں ضروری ہے۔
- بچوں کو اپنے ذاتی ڈیٹا کی حفاظت اور اسے اجنبیوں کی رسائی میں نہ دینے کی اہمیت کے بارے میں بتائیں۔
- بچوں کو بتائیں کہ اجنبی ہمیشہ سچ نہیں بولتے۔ اس لیے ان پر اعتبار نہیں کیا جا سکتا ہے۔
- اپنے بچے کی موجودگی میں پرائیویسی کی سیٹنگز میں جا کر تبدیلی کریں تاکہ آپ کا بچہ یہ نہ سمجھے کہ اس پر یہ سب کچھ زبردستی مسلط کیا جا رہا ہے۔

- اپنے بچوں کو وضاحت کریں کہ ان احتیاطی تدابیر کا مقصد ان کی سرگرمی کو محدود کرنا نہیں ہے۔ اس کے بجائے ان کا مقصد انھیں لوگوں کے ممکنہ منفی رویے سے محفوظ رکھنا ہے۔
- اپنے بچے کے سوشل میڈیا کے استعمال سے متعلق بنیادی اصول بنائیں۔ جیسے یہ کہ کتنے گھنٹے وہ اسے استعمال کر سکتا ہے اور دن کا کون سا حصہ اس مصروفیت کے لیے موزوں ہو گا، وغیرہ۔ لیکن کوشش کریں کہ یہ اصول وضع کرنے کے عمل میں ان کی منشا بھی شامل رکھیں۔ نہ کہ تحکمانہ رویے کے ساتھ یہ اصول ان پر نافذ کرنے کی کوشش کریں۔ اسی طرح چند اصول والدین کے لیے بھی بنائیں اور مثال قائم کرنے کے لیے ان کی پیروی کریں۔
- احتیاطی تدابیر جیسے مال ویئر کی سکیننگ کروانے کی حوصلہ افزائی کے لیے ترغیبات دیں جیسے انٹرنیٹ کے استعمال کے لیے کچھ مزید وقت بچے کو دیں۔
- ان کی جاسوسی مت کریں۔ اپنے بچوں پر ہمیشہ نظر رکھنے کے بجائے انھیں سوشل نیٹ ورک کے آداب سمجھانے کی کوشش کریں۔ اس سے آپ کے باہمی رشتے میں اعتماد پیدا ہو گا اور آپ کے بچے کسی بھی مشکل صورت حال میں آپ سے رجوع کرنے میں آسانی محسوس کریں گے۔



کام کی بات: اپنے بچوں کو سکھائیں کہ اجنبیوں کو یہ معلومات یعنی چار 'پ' نہ دیں۔

سوشل میڈیا پر اپنے بچے کی پرائیویسی کا تحفظ کریں

آج کل سوشل میڈیا کے صارفین کی بڑی تعداد وہاں اپنے بچے کی تصاویر اور دیگر تفاصیل فراہم کرتے ہیں۔ بعض اوقات بچے کے پیدا ہونے سے بھی پہلے کی معلومات دی جاتی ہیں۔ اپنے بچے کی پیدائش سے بھی پہلے اس کے نام سے سوشل میڈیا میں اکاونٹس کھولنے سے ایک ڈیجیٹل نقش پیدا کر کے غلط نتائج نکل سکتے ہیں۔ ضروری نہیں ہے کہ مستقبل میں پیدا ہونے والا بچہ واقعی اس سب کچھ کی اجازت دے۔ اسی طرح نومولود بچے بھی اپنے والدین کی طرف سے سوشل میڈیا پر ان کی تصویریں شائع کرنے پر اپنی رضامندی یا نارضامندی کا اظہار نہیں کر سکتے ہیں۔

کام کی بات: اگر آپ کے بچے انکار یا اقرار نہیں کر سکتے تو ان کی تصویریں مدھم کر دیں۔ اسی طرح یہ بات ذہن نشین رکھیں کہ اگر آپ کے رشتہ دار یا دوست بچے کی تصویر لینے کی کوشش کریں تو انھیں انکار کر دیں۔

پرائیویسی کا مطلب رازداری نہیں ہے

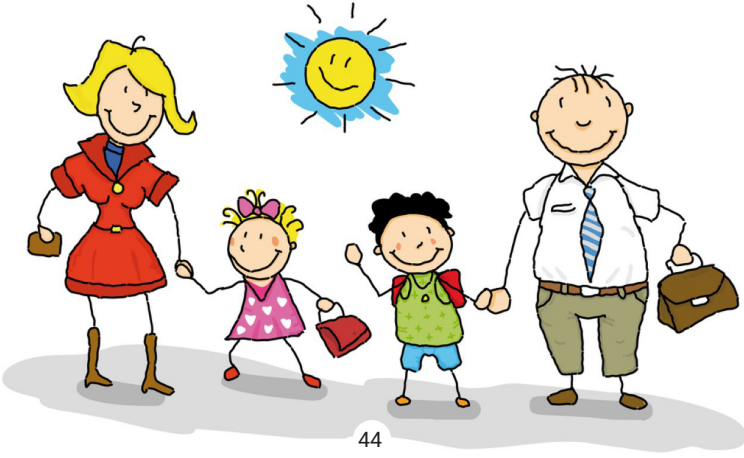
کیا آپ گلیوں میں اجنبیوں کو اپنے رازوں سے آگاہ کرتے ہیں اور ان کو اپنی ذاتی معلومات فراہم کرتے ہیں؟ اگر نہیں تو پھر آن لائن ایسا کرنے کی بھی کوئی وجہ نہیں ہے۔

پرائیویسی کو رازداری سے گڈمڈ نہیں کرنا چاہئے۔ اگر آپ رات کو اپنے گھر کے دروازے بند کر لیتے ہیں تو اس کا یہ مطلب نہیں ہے کہ آپ پراسرار ہیں۔ آپ صرف اپنی پرائیویسی کو برقرار رکھنا چاہتے ہیں۔ یہ اصول آن لائن جگہوں پر بھی لاگو ہوتا ہے۔ اگر آپ آن لائن کچھ شیئر کرتے اور کچھ شیئر نہیں کرتے ہیں، تو اس سے بھی آپ پراسرار ثابت نہیں ہوتے۔ اس کا مطلب صرف یہ ہے کہ آپ اپنی پرائیویسی کو قائم رکھنا چاہتے ہیں۔

ایک اچھی مثال قائم کرنا

بچوں اور نوجوانوں میں سیکھنے کی اہلیت غیر معمولی ہوتی ہے اور وہ آس پاس لوگوں کے رویوں کی نقل کرتے ہیں۔ بچوں میں صحت مندانہ عادتیں پیدا کرنے کے لیے رول ماڈلز بہت اہم کردار ادا کرتے ہیں۔ مثال کے طور پر اگر آپ کا بچہ آپ کو دیکھتا ہے کہ آپ پرائیویسی کا لحاظ کیے بغیر خاندان کی تصویریں سوشل میڈیا میں پیش کرتے ہیں تو وہ بھی پرائیویسی کا لحاظ رکھنے کی طرف کم ہی مائل ہو گا۔ جو آپ تبلیغ کرتے ہیں، اس پر عمل بھی کریں۔

اپنے بچوں سے متعلق کوئی بات پوسٹ کرنے سے پہلے ان سے پوچھیں۔ چاہے وہ چھٹیوں کے دن کی تصویر ہو یا ان کے امتحانوں کے رزلٹ کارڈ کی تصویر۔



حوالہ جات

https://www.childnet.com/resources
https://www.saferinternet.org.uk/advice-centre/parents-and-carers
https://www.esafety.gov.au/parents
https://www.commonsensemedia.org/
https://bullyingnoway.gov.au/RespondingToBullying/GetHelpandMoreInformation/Pages/Online-safety.aspx
https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/online-safety/talking-your-child-staying-safe-online/

DigitalRightsFoundation

"KNOW YOUR RIGHTS"

Supported by

FRIEDRICH NAUMANN FOUNDATION For Freedom.

Pakistan