سوشل میڈیا کا محفوظ استعمال

پی ٹی اے کی رہنما ہدایات برائے آن لائن تحفظ

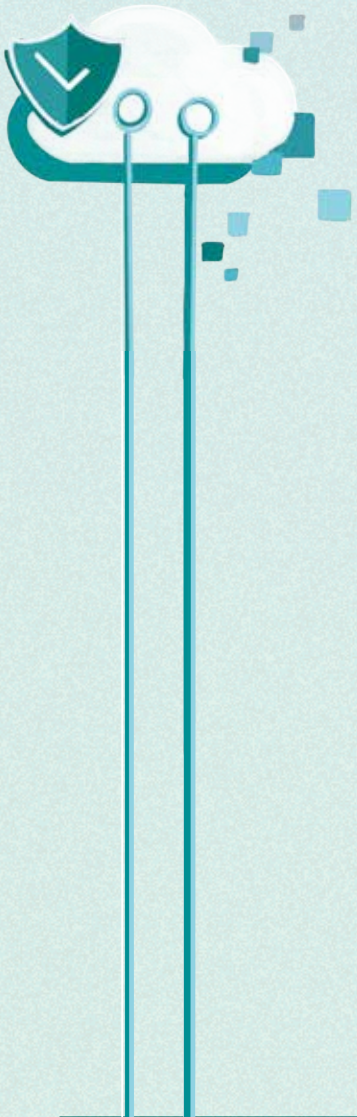
پاکستان ٹیلی کمیونیکیشن اتھارٹی

pta.gov.pk PakistanTelecommunicationAuthority PTAOfficialPK @PTAofficialpk

اشاعت کار
تصنیف و ادارت
شعبہ تعلقات عامہ
پاکستان ٹیلی کمیونیکشن اتھارٹی
ہیڈ کوارٹرز ,F-5/1 اسلام آباد، پاکستان
ویب سائٹ :www.pta.gov.pk

اشاعتی ڈیٹا میں فہرست سازی
پاکستان ٹیلی کمیونیکشن اتھارٹی
سوشل میڈیا کا محفوظ استعمال۔رہنما ہدایات برائے آن لائن تحفظ
ISBN: 978-969-8667-63-4

فہرست



انٹرنیٹ کا محفوظ استعمال کیوں اہم ہے؟

عوام الناس کی روزمرہ سرگرمیوں میں ڈیجیٹل ٹیکنالوجی کا استعمال اب عام ہو چکا ہے۔ درحقیقت زندگی کے آن لائن معاملات بھی آف لائن معاملات کی طرح انتہائی اہمیت کے حامل ہیں۔ یہ کتابچہ نوجوانوں اور بچوں کو آن لائن درپیش ممکنہ نقصانات کے حوالے سے رہنما ہدایات پر مشتمل ہے جس میں آن لائن ذرائع کا محفوظ اور ذمہ دارانہ استعمال اور مثبت ڈیجیٹل فٹ پرنٹ کو برقرار رکھنے کے لئے اٹھائے جانے والے اقدامات بھی شامل ہیں ۔

آن لائن مواد کیا ہے؟

تصویر، ویڈیو یا متن پر مبنی کوئی بھی مواد جو آن لائن اپ لوڈ اور شیئر کیا جائے آن لائن مواد کہلاتا ہے۔ اگرچہ آن لائن مواد کی نوعیت جہاں مثبت ہے وہیں بہت سا مواد ایسا بھی ہے جو آپ کے لئے پریشانی یا جذباتی نقصان کا باعث بن سکتا ہے۔آن لائن دنیا اب غلط سرگرمیوں میں ملوث افراد کی طرف سے غیر قانونی اور نقصان دہ سرگرمیوں کے طور پر بھی استعمال کی جا رہی ہے۔

غیر قانونی مواد

کتابچے کے اس جزو میں نوجوان نسل کو غیر قانونی ، نقصان دہ، گستاخانہ اور فحش آن لائن مواد کی پہچان اور اس سے بچاؤ کے حوالے سے رہنما ہدایات شامل کی گئی ہیں ۔ پاکستانی قانون کے مطابق غیر قانونی آن لائن مواد کی فہرست اگلے صفحات میں موجود ہے۔

گستاخانہ مواد

بعض دفعہ آف لائن زندگی کی طرح جب آپ آن لائن ہوتے ہیں تو آپ کے سامنے ایسا مواد آ سکتا ہے جو آپ کے لئے پریشان کن، اشتعال انگیز اور خلاف روایت ثابت ہو سکتا ہے۔

''کسی بھی مذہب'' کی توہین اور ''عظمت اسلام'' کے خلاف مواد پاکستان پینل کوڈ، 1860 کے باب XV (ایکٹ XLV,1860) (''پی پی سی'') کے تحت ایک قابل سزا جرم ہے۔ مزید برآں پی پی سی کی دفعہ 295 سی کے تحت نبی کریم صلی اللہ علیہ وآلہ وسلم کے مقدس نام کی بے حرمتی کے مرتکب شخص کو سزائے موت یا عمر قید کی سزا دی جائے گی اور جرمانہ بھی عائد کیا جائے گا۔

نفرت آمیز تقاریر

آن لائن نفرت کی تعریف نسل، مذہب ،لسانیت، معذوری یا جنسی بنیادوں پر کسی شخص یا طبقے کے بارے میں نفرت آمیز پوسٹ کے طور پر کی جا سکتی ہے۔ پریوینشن آف الیکٹرانک کرائم ایکٹ (پی ای سی اے) 2016 میں سوشل میڈیا پر نفرت آمیز تقاریر کی وضاحت اس طرح سے ہے ''وہ معلومات جو معلوماتی نظام یا ڈیوائس کے ذریعے بین المذاہب ، فرقہ واریت یا لسانی منافرت کے امکان کو بڑھائے یا بڑھانے کی صلاحیت رکھتی ہو''۔
یہ قانون معاشرے میں بسنے والے گروہوں اور طبقات کے تحفظ کے لیے بنایا گیا ہے۔ وہ نوجوان زیادہ تر آن لائن نفرت کا شکار ہوتے ہیں جو

- اپنی شناخت کے متلاشی ہوں
- گھر والوں کو درپیش کسی مسئلے یا تکلیف دہ واقعے یا سوگ کا سامنا کر رہے ہوں
- معذوری، فرقہ وارانہ یا لسانی امتیازی سلوک کا سامنا ہو

انٹرنیٹ پر موجود مواد کی غیر معتبر نوعیت کے پیش نظر اس کے واضح اثرات فوری طور پر سامنے نہیں آتے لہذا صارفین کی تعداد ایسی بھی ہے جو بغیر کسی روک و ٹوک اپنے ناخوشگوار و نفرت آمیز آراء اور ردعمل کا اظہار کرتی نظر آتی ہے۔ جس کے منفی اثرات دیگر قارئین پر بھی پڑتے ہیں۔

نامناسب / غیر اخلاقی مواد

فلموں، میوزک ویڈیوز، آن لائن گیمز یا اشتہارات جو ایسے فحش / جنسی طور پر نازیبامواد پر مشتمل ہوں جن سے آپ کو اس کے نقصان دہ یا منفی ہونے کا تاثر ملے جیسا کہ :۔

- ✕ غیر حقیقت پسندانہ تعلقات کی توقعات وابستہ کر لینا
- ✕ باہم رضامندی شامل نہ ہونا
- ✕ خواتین کے ساتھ بدسلوکی اور پر تشدد سلوک

جنسی زیادتی اور استحصال کا شکار بچوں کی تصاویر اور غیر اخلاقی ویڈیوز (چـائلڈ پورنو گرافی) بنانا، مہیا کرنا اور نشر کرنا سنگین جرم ہے۔

ریاست مخالف مواد

پی ای سی اے (2016) کے تحت پاکستان کی سالمیت، دفاع یاپبلک آرڈر(امن عامہ) کے خلاف مواد اپ لوڈ یا شیئر کرنا غیر قانونی ہے۔

پاکستان کے آئین 1973 کے آرٹیکل 19 کے تحت، اظہار رائے کی آزادی معقول پابندیوں کے ساتھ ہے ۔تاہم تشدد پر اُکسانے، نفرت آمیز تقاریر کو فروغ دینے اور امن عامہ کے لیے خطرہ بننے والی غلط معلومات پھیلانے والے گروہوں اور افراد کو ایسا کرنے کی اجازت نہیں دی جا سکتی۔

ہتک عزت (بدنامی)

انٹرنیٹ پر ہتک عزت ''دانستہ طور پر اور بظاہر''کسی بھی ایسی معلومات کو ظاہر کرنا یا پہنچانا ہے جو ''غلط'' ہے اور اس سے کسی شخص کی پرائیویسی کو نقصان پہنچ سکتا ہے (پی ای سی اے 2016 ، سیکشن 20)۔

اس طرح کے آن لائن حملے نوجوانوں اور ان کی شخصیت پر منفی اثرات مرتب کر سکتے ہیں ۔بعض دفعہ ایسے حالات میں انہیں اپنے قانونی حقوق سے بھی آگاہی نہیں ہوتی۔ اگر کوئی آپ کو آن لائن پریشان کر رہا ہے توآپ ذیل سے رہنمائی حاصل کر سکتے ہیں:۔

- تصویر/ویڈیو یا تحریری پوسٹ کے اسکرین شاٹس لیں اور مواد کو ہٹانے کے لئے سوشل میڈیا پلیٹ فارم کو براہ راست رپورٹ کریں۔

- برائے تفتیش قانون نافذ کرنے والے متعلقہ ادارے کو رپورٹ کریں۔

نقصان دہ آن لائن مواد کی دیگر اقسام

اگرچہ مندرجہ ذیل مواد غیر قانونی نہیں ہے،لیکن اس کا آن لائن فروغ نقصان دہ ثابت ہوسکتا ہے لہٰذا کسی بھی قسم کی زحمت سے بچنے کے لئے اس طرح کے مواد کی فوری طور پر نشاندہی ثابت کریں ۔

جعلی خبریں (فیک) نیوز

جعلی خبروں سے مراد ایسی خبروں کا آن لائن فروغ ہے جو جھوٹی، گمراہ کن یا غلط حقائق پر مبنی ہوتی ہیں لیکن بظاہر کسی بھی صورت حال کی درست نمائندگی کرتی دکھائی دیتی ہیں۔

جعلی خبروں کا پرچار کرنے والی ویب سائٹس اور پیجز مناسب نیوز سائٹس کی طرح نظر آنے کے لیے ٹیکنالوجی اور سوشل میڈیا جیسے ذرائع استعمال کرتی ہیں۔ ہیکرز متعدد سوشل میڈیا اکاونٹس بنانے کے لئے بوٹس (Bots) اور سافٹ ویئر کا استعمال کرتے ہیں اور ان کا استعمال غلط حقائق پر مبنی خبریں پھیلانے کے لئے کرتے ہیں۔

بعض اوقات صحافیوں کی جانب سے بھی گمراہ کن معلومات فراہم کی جاتی ہیں جس کی وجہ سے اصل حقائق تک رسائی مشکل ہو جاتی ہے۔

حقیقت کو بے نقاب کریں

کسی بھی موصول ہونے والی خبر کے بارے میں تنقیدی سوالات پوچھیں اور اس بات کی تصدیق ضرور کریں کہ آیا خبرصحیح ہے یا غلط۔

- ویب سائٹ کون سی ہے؟
- یہ کس نے لکھا (اور کب)؟
- پورا مضمون یا ویڈیو کیا کہتا ہے؟
- کن ذرائع کا حوالہ دیا جا رہا ہے ؟

صارف کی جانب سے تخلیق کردہ نقصان دہ مواد

سوشل میڈیا پر دوسرے صارفین کی تصاویر اور ویڈیوز ان کی حقیقی زندگی کی عکاسی کرتی نظر آتی ہیں۔ جبکہ زیادہ تر وقت وہ آپ کو ایسا طرز زندگی دکھا رہے ہوتے ہیں جس کا تصور محض خیالی دنیا میں ہی ممکن ہے۔

ہر فرد اپنی شخصیت کو آن لائن سطح پر بناوٹی انداز میں ایسے پیش کر سکتا ہے جس میں وہ اپنی زندگی کے سب سے بہترین پہلو نمایاں کرے۔
سوشل میڈیا کا دباؤ حقیقی ہے اور اس کے نتائج نوجوانوں سمیت سب کے لیے یکساں ہیں۔ بسا اوقات ایسا مواد کسی شخص کو خطرناک رویہ اختیار کرنے یا نقصان دہ اور دقیانوسی ردعمل کی جانب راغب کر سکتا ہے۔

تمام سوشل میڈیا پلیٹ فارمز کی جانب سے کمیونٹی کے رہنما اصول و ضوابط (گائیڈ لائنز) بنائے گئے ہیں، جس میں پریشان کن یا دھمکی آمیز رویے کے خلاف، تشدد پر مبنی تصاویر اور ویڈیوز، اور ہیکنگ کی معلومات کی فراہمی کی روک تھام شامل ہے۔

کمیونٹی گائیڈلائنز کیا ہیں؟

کمیونٹی گائیڈ لائنز سوشل میڈیا پلیٹ فارم کی جانب سے بنائے گئے قوانین کا ایک مجموعہ ہے تاکہ صارفین کے لیے محفوظ ماحول پیدا کرتے ہوئے متعلقہ پلیٹ فارم پر معیاری و مثبت طرز عمل کو یقینی بنایا جا سکے۔ کمیونٹی گائیڈ لائنز ایسے ممنوعہ مواد کا احاطہ کرتے ہیں جو غیر قانونی اور ناپسندیدہ سرگرمیوں پر اکاؤنٹس کو معطل یا مستقل طور پر ڈیلیٹ کرنے کا باعث بن سکتی ہیں۔

ہدایات پر عمل پیرا نہ ہونے کے نتائج

ان ہدایات پر عمل پیرا نہ ہونے کے نتائج اکاؤنٹ کی معطلی یا اس کا مستقل طور پر ڈیلیٹ ہو جانا بھی ہو سکتے ہیں۔ اس بات کو یقینی بنانے کے لئے کہ آپ پلیٹ فارم کی ہدایات پر عمل پیرا ہیں، ان کا جائزہ لیں تاکہ آپ کو معلوم ہو کہ پوسٹ کرنے سے پہلے کون سا مواد قابل قبول سمجھا جاتا ہے۔ آپ کی رہنمائی کے لئے ذیل میں مقبول سوشل میڈیا پلیٹ فارمز سے کمیونٹی کے رہنمااصول* دیئے گئے ہیں:۔

انسٹاگرام	https://help.instagram.com/477434105621119
فیس بک	https://www.facebook.com/help/477434105621119/?helpref=uf_share
سنیپ چیٹ	https://snap.com/ur-PK/community-guidelines
ڈسکارڈ	https://discord.com/guidelines
ٹک ٹاک	https://www.tiktok.com/community-guidelines?lang=ur
یوٹیوب	https://www.youtube.com/howyoutubeworks/policies/community-guidelines/
ٹوئٹر	https://help.twitter.com/en/rules-and-policies/twitter-rules

*ان رہنما ہدایات میں وقتاً فوقتاً ترمیم ہوسکتی ہیں

رپورٹ کرنے کا طریقہ کار

بلاک، ڈیلیٹ اور ان فالو کریں

اگر کوئی شخص آپ کو مسلسل ایسا مواد بھیج رہا ہے جو آپ نہیں دیکھنا چاہتے۔ اسے بلاک، ان فالو یا ڈیلیٹ کردیں۔

سوشل میڈیا پلیٹ فارمز پر رپورٹنگ

مختلف پلیٹ فارمز کے رپورٹنگ فیچرز بھی اس حوالے سے سہولت مہیا کرتے ہیں جس کے ذریعے صارف پریشان کن یا نقصان دہ پروفائلز، ویڈیوز ، تصاویر وغیرہ پرمشتمل مواد رپورٹ کرے۔

بعض اوقات رپورٹ کی نوعیت کے لحاظ سے سوشل میڈیا پلیٹ فارمز آپ سے ایک فارم پُر کرنے اور چند ذاتی سوالات کے جوابات دینے کے لیے بھی کہہ سکتے ہیں۔ مثال کے طور پر، اگر آپ کسی ایسے شخص کی اطلاع دے رہے ہیں جو آپ کی یا کسی جاننے والے کی فیک آئی ڈی استعمال کر رہا ہے، تو وہ آپ سے شناخت کی تصدیق کے لیے اسکین شدہ دستاویزات بھیجنے کے لیے کہہ سکتے ہیں۔

ذیل میں مقبول ترین سوشل میڈیا پلیٹ فارمز کے لنکس دیے گئے ہیں تاکہ آپ ایسے ناپسندیدہ مواد کی اطلاع دے سکیں جو کمیونٹی کے رہنما اصولوں کے خلاف ہیں۔

فیس بک	https://www.facebook.com/help/181495968648557
انسٹاگرام	https://help.instagram.com/519598734752872
ٹک ٹاک	https://support.tiktok.com/en/safety-hc/report-a-problem/report-a-video
ٹوئٹر	https://help.twitter.com/en/rules-and-policies/twitter-report-violation#specific-violations
یوٹیوب	https://support.google.com/youtube/answer/2802027?hl=en&co=GENIE.Platform%3DAndroid
سنیپ چیٹ	https://support.snapchat.com/en-US/i-need-help
ڈسکارڈ	https://support.discord.com/hc/en-us/requests/new

پاکستان میں انٹرنیٹ سے متعلقہ قوانین

پی ای سی اے 2016

پریوینشن آف الیکٹرانک کرائمز ایکٹ 2016(پی ای سی اے) کا نفاذ 22 اگست، 2016 کو عمل میں لایا گیا۔ یہ قانون الیکٹرانک جرائم پر مبنی غیر قانونی سرگرمیوں کی روک تھام کے حوالے سے بنایا گیا اور اس میں متعلقہ جرائم کے ساتھ ساتھ ان کی تحقیقات، استغاثہ، مقدمے کی سماعت اور بین الاقوامی تعاون وغیرہ کے لئے بھی عملی طریقہ کار وضع کیا گیا ہے۔

غیر قانونی آن لائن مواد کو ہٹانا اور بلاک کرنا (طریقہ کار، نگرانی اور تحفظ) کے قواعد، 2021

یہ قواعد جن کو عام زبان میں "سوشل میڈیا رولز" بھی کہا جاتا ہے 12 اکتوبر 2021 کو گزٹ نوٹیفائی کیے گئے جس میں اہم سوشل میڈیا کمپنیوں کی رجسٹریشن اور شکایات کے ازالے کے طریقہ کار اور پی ای سی اے کے تحت غیر قانونی آن لائن مواد تک رسائی کی روک تھام اور اسے ہٹانے کی حکمت عملی وضع کی گئی ہے۔

پی ای سی اے ایکٹ 2016 کے تحت پی ٹی اے کا کردار

پی ای سی اے کے سیکشن 37 کے تحت پی ٹی اے کو پاکستان میں کسی بھی انفارمیشن سسٹم کے ذریعے پھیلائے جانے والے غیر قانونی آن لائن مواد کو بلاک کرنے/ہٹانے کا اختیار ہے۔ اس میں پاکستان کے دفاع یا سلامتی (ریاست مخالف)، عظمت اسلام کے خلاف (توہین آمیز)، نفرت آمیز تقاریر (پبلک آرڈر)، غیر اخلاقی اور غیر مہذب مواد (فحش)، توہین عدالت، ہتک عزت/ نقالی پر مبنی مواد شامل ہے۔

شکایات کا طریقہ کار

بلاک کرنے کے لیے

کوئی بھی شخص پی ٹی اے کے ای میل ایڈریس

content-complaint@pta.gov.pk

یا کمپلینٹ مینجمنٹ سسٹم

https://complaint.pta.gov.pk/RegisterComplaint.aspx

یا پی ٹی اے سی ایم ایس موبائل ایپ کے ذریعے غیر قانونی آن لائن مواد کو بلاک کرنے کے لئے شکایات کا اندراج کر سکتا ہے۔

شکایت موصول ہونے پر پی ٹی اے لنک کو بلاک / ڈیلیٹ کرنے کے لیے کارروائی کرتا ہے اور شکایت کنندہ کو حتمی نتائج سے بھی آگاہ کر دیا جاتا ہے۔ پی ٹی اے گستاخانہ، فحش مواد یا پاکستان کی سلامتی و دفاع کے خلاف استعمال ہونے والے لنکس بھی بلاک کر رہا ہے۔

برائے تفتیش

آن لائن جرائم سے متعلق سائبر کرائم ونگ، فیڈرل انویسٹی گیشن ایجنسی کو رپورٹ کریں۔

ہیلپ لائن : 1991

ای میل : helpdesk@nr3c.gov.pk

ویب سائٹ : https://www.fia.gov.pk/ccw

اس گائیڈ تک آن لائن رسائی اور پی ٹی اے کی رہنما ہدایات برائے آن لائن تحفظ سے متعلقہ مزید معلومات کے لئے یہ کوڈ اسکین کریں۔

پریوینشن آف الیکٹرانک کرائمز ایکٹ (پی ای سی اے) 2016	
تفصیل	متعلقہ سیکشن اور اختیارات
ایکٹ کا نام	پریوینشن آف الیکٹرانک کرائمز ایکٹ (پی ای سی اے)
دیباچہ	میکانزم برائے i) تحقیقات، ii) استغاثہ، iii) مقدمے کی سماعت اور iv) الیکٹرانک جرائم کے ضمن میں بین الاقوامی معاونت
کل سیکشن	پچپن (55)

پی ای سی اے 2016 میں جرائم کا خلاصہ					
نمبر شمار	دفعات	جرائم کی تفصیل	پی ای سی اے کے تحت سزا		
			جرمانہ	قید	
1	سیکشن 3	معلوماتی نظام یا ڈیٹا تک غیر مجاز رسائی	پچاس ہزار	تین ماہ	یا دونوں
2	سیکشن 4	ڈیٹا کی غیر مجاز نقل یا ترسیل	ایک لاکھ	چھ ماہ	یا دونوں
3	سیکشن 6	کریٹیکل انفراسٹرکچر انفارمیشن سسٹم یا ڈیٹا تک غیر مجاز رسائی	دس لاکھ	تین سال	یا دونوں
4	سیکشن 7	کریٹیکل انفراسٹرکچر انفارمیشن سسٹم یا ڈیٹا کی غیر مجاز نقل	پچاس لاکھ	پانچ سال	یا دونوں
5	سیکشن 9	کسی جرم کی ترغیب	ایک کروڑ	سات سال	یا دونوں
6	سیکشن 10	سائبر حملہ	پانچ کروڑ	چودہ سال	یا دونوں
7	سیکشن 11	نفرت آمیز تقاریر	موجود نہیں	سات سال	یا دونوں
8	سیکشن 12	دہشت گردی کے مقاصد کے پیش نظر خریداری، فنڈنگ اور منصوبہ بندی	موجود نہیں	سات سال	یا دونوں

پی ای سی اے 2016 میں جرائم کا خلاصہ				
نمبر شمار	دفعات	جرائم کی تفصیل	پی ای سی اے کے تحت سزا	
			جرمانہ	قید
9	سیکشن 13	الیکٹرانک جعل سازی	دو لاکھ پچاس ہزار	تین سال	یا دونوں
10	سیکشن 14	الیکٹرانک دھوکہ دہی	ایک کروڑ	دو سال	یا دونوں
11	سیکشن 15	کسی بھی جرم میں استعمال کے لئے ڈیوائس کی بناوٹ، حصول یا فراہمی	پچاس ہزار	چھ ماہ	یا دونوں
12	سیکشن 16	ذاتی معلومات کا غیر مجاز استعمال	پچاس لاکھ	تین سال	یا دونوں
13	سیکشن 17	سم کارڈز کا غیر مجاز استعمال	پانچ لاکھ	تین سال	یا دونوں
14	سیکشن 20	شخصی وقار کے خلاف جرائم	دس لاکھ	تین سال	یا دونوں
15	سیکشن 21 (1)	کسی شخص اور نابالغ کی عفت کے خلاف جرم	پچاس لاکھ	پانچ سال	یا دونوں
16	سیکشن 22	چائلڈ پورنو گرافی (بچوں سے غیر اخلاقی سلوک پر مبنی مواد)	پچاس لاکھ	سات سال	یا دونوں
17	سیکشن 23	نقصان دہ کوڈ	دس لاکھ	دو سال	یا دونوں
18	سیکشن 24	سائبر ہراسانی	دس لاکھ	تین سال	یا دونوں
19	سیکشن 25	ان چاہے پیغامات (سپیمنگ)	پچاس ہزار جو کہ بڑھ کر دس لاکھ ہو سکتی ہے	تین ماہ	یا دونوں
20	سیکشن 26	جعل سازی (سپوفنگ)	پانچ لاکھ	تین سال	یا دونوں

دفعات برائے تعزیرات پاکستان (پی پی سی)			
نمبر شمار	دفعہ	تفصیل	سزائیں
1	دفعہ 295 اے	دانستہ اور معاندانہ افعال جس کا منشا کسی فرقے کے مذہبی احساسات کی، اس کے مذہب یا عقائد کی توہین کر کے بے حرمتی کرنا ہو۔	دس(10) سال قید یا جرمانہ یا دونوں
2	دفعہ 295 بی	قرآن پاک کی بے حرمتی	عمر قید
3	دفعہ 295 سی	نبی کریم ﷺ کے خلاف توہین آمیز کلمات	سزائے موت یا عمر قید اور جرمانہ
4	دفعہ 298	توہین آمیز کلمات کے ذریعے مذہبی جذبات کو ٹھیس پہنچانا	ایک(01)سال تک قید یا جرمانہ یا دونوں
5	دفعہ 298 اے	مقدس ہستیوں کے خلاف تضحیک آمیز کلمات	تین(03)سال تک قید یا جرمانہ یا دونوں
6	دفعہ 298 بی	ان القابات و خطابات اور توصیف وغیرہ کا غلط استعمال جو تقدس مآب شخصیات اور مقامات کے لئے مخصوص ہوں۔	تین(03)سال تک قید یا جرمانہ یا دونوں

آن لائن گرومنگ

ایسا بھی ہو سکتا ہے کہ آپ کا کسی سے آن لائن رابطہ ہواور جیسا اس نے آپ کو اپنی شخصیت کے بارے میں بتایا ہو گا حقیقت اس کے بالکل برعکس ہو۔ انٹرنیٹ کے ذریعے نوجوانوں اور بچوں کا جنسی استحصال گرومنگ کہلاتا ہے ۔

آن لائن گرومنگ کیسے ہوتی ہے؟

نوجوان افراد بسا اوقات دھوکہ باز لوگوں پر بھروسہ کر بیٹھتے ہیں جن کے بارے میں درحقیقت وہ کچھ جانتے ہی نہیں۔

آن لائن گرومرز بعض اوقات اپنی اصل شناخت چھپا کر اپنے آپ کو کوئی اور ظاہر کر سکتے ہیں۔	اپنے اور متاثرہ افراد کے مابین اعتماد کی فضا	گرومر ایسا شخص بھی ہو سکتا ہے جسے آپ پہلے سے ہی جانتے ہوں
گرومرز نوجوانوں میں مقبول سوشل میڈیا پلیٹ فارمز کا استعمال کرتے ہیں اور ایسا ظاہر کرتے ہیں جیسے یہ انہی میں سے ایک ہیں۔ ایسے افراد اپنے شکار کا انتخاب اس کی نفسیاتی کمزوری کو جانچ کر کرتے ہیں۔ وہ ایسا ظاہر کرتے ہیں جیسے ان کے عادات اور مشاغل تشابہ ہیں، وہ کسی اور کی تصاویر کا استعمال کرتے ہیں یا تحائف، فالوورز یا "راز" شیئر کرنے کا دکھاوا کرتے ہیں۔	ایک بار متاثرہ شخص کا اعتماد حاصل کر لینے کے بعد گرومرز نوجوان شخص سے نازیبا تصاویر یا ویڈیوز طلب کر سکتے ہیں۔ وہ متاثرہ شخص کو جذباتی طور پر بلیک میل کرنے کی کوشش کریں گے اور بات نہ ماننے پر بلاک کرنے کی دھمکی دیں گے۔ متاثرہ شخص ایسی صورتحال کے دوران خود کو بے بس محسوس کر سکتا ہے اور اپنی ذاتی تصاویر شیئر کر سکتا ہے۔ جن کا بعد میں گرومرز منفی استعمال کر سکتے ہیں۔	آن لائن گرومر کوئی بھی ایسا شخص ہو سکتا ہے جس کو متاثرہ شخص پہلے ہی اپنے کنبہ یا سماجی حلقہ احباب کے ذریعے مل چکا ہوتا ہے۔ وہ اپنے شکار کے ساتھ تعلقات قائم کرنے کے لئے انٹرنیٹ کا بھرپور استعمال کرتے ہیں۔ گرومرز شخصی طور پر پرکشش، مہربان اور کبھی کبھار آپ کے لئے مددگار ثابت ہونے کا ڈرامہ کر سکتا ہے۔ اس کے برعکس کسی کے وہم و گمان میں بھی نہیں ہوتا کہ اسے ذہنی طور پر "گروم" کیا جارہا ہے۔

آن لائن گرومنگ کیسے ممکن ہے؟

آن لائن گرومرز / شکاری بچوں اور نو عمر افراد کو ایسی ویب سائٹس، پلیٹ فارمز اور ایپس کے ذریعے نشانہ بنا سکتے ہیں جو نوجوانوں میں مقبول ہیں (اس میں جاب فورم اور گیمنگ سائٹس بھی شامل ہیں)۔ایسا شخص دوسرے فرد کے سامنے اُس کے ہم عمر کے طور پر ظاہر ہو سکتا ہے۔ شکاری اعتماد حاصل کرنے کے لئے بات چیت کا آغاز دوستانہ طریقے سے کرے گا۔اس کے بعد وہ اپنے شکار سے چیٹ کرنے کے لئے اس کا ذاتی فون نمبر مانگے گا۔

خطرے کی علامات

آپ سے آن لائن رابطہ کرنے والا شخص آپ کے لئے اجنبی یا کوئی بھی ایسا شخص ہو سکتا ہے جسے آپ پہلے سے ہی جانتے ہیں یا مل چکے ہیں۔ وہ کوئی ایسا شخص بھی ہو سکتا ہے جو آپ سے عمر میں بڑا یا ہم عمر ہو سکتا ہے۔آپ پر نظر رکھنے والا شخص اپنی جنس ، رہائش اور اصل عزائم سے متعلق آپ کے سامنے جھوٹ کا سہارا لے سکتا ہے ۔ ذیل میں خطرے کی چند علامات ملاحظہ فرمائیے:-

- **آپ خود کو پریشان محسوس کریں گے** ۔ شکار کرنے والا فرد اپنی بھرپور کوشش کرے گا اور اپنے شکار سے اہم سوالات کرے گا ۔ ایسے میں اپنی صلاحیتوں کا استعمال کریں۔

- **وہ آپ کو بتائے گا کہ اس کی ویب کیم یا ویڈیو ایپ کام نہیں کر رہی ہے**۔ آن لائن گرومر اپنے آپ کو آپ کے سامنے کوئی اور ظاہر کر سکتا ہے۔ وہ کہے گا کہ ان کا ویب کیم یا ویڈیو ایپ کام نہیں کر رہا ہے تاکہ آپ نہ دیکھ پائیں کہ وہ ظاہری طور پر کیسا نظر آتا ہے۔

- **وہ آپ کی ظاہری شکل و صورت یا جسامت سے متعلق نامناسب باتیں کریں گے** ۔ اور آپ یا آپ کے خاندان کے دیگر ممبران / دوستوں کی ذاتی تصاویر طلب کریں گے ۔ کسی بھی ایسے شخص کے آن لائن رویے سے محتاط رہیں جو بلاوجہ آپ کی بے تحاشا تعریفیں کرے۔

- **وہ آپ سے متعدد بار اور مختلف طریقوں سے رابطہ کرنے کی کوشش کرتے ہیں** ۔ مثال کے طور پر، آپ کی ان سے ریڈٹ (ویب ایپ) پر ملاقات ہوتی ہے وہ آپ کا فون نمبر پوچھنے کے بعد آپ سے براہ راست پیغام رسانی کا سلسلہ شروع کر دیتے ہیں۔

- **وہ ملاقات پر اصرار کرتے ہیں اور ذاتی طور پر ملنے کا کہتے ہیں** ۔ انکار کی صورت میں آپ پر غصہ / ناراضگی کا اظہار کریں گے اور آپ کو " بُرا دوست " کہیں گے ۔

- **وہ اس تعلق کو خفیہ رکھنا چاہتے ہیں** ۔ جو لوگ آپ کو نقصان پہنچانا چاہتے ہیں وہ نہیں چاہتے کہ دوسرے لوگوں کو اس تعلق کا علم ہو ۔ وہ آپ سے کہتے ہیں کہ آپ صرف اس وقت اُن سے رابطہ کریں جب آپ تنہا ہوں ۔

- **وہ آپ سے رقم یا اپنے کسی کام کے بارے میں بات کرے گا**۔ آپ کا اعتماد حاصل کر لینے کے بعد گرومر آپ سے رقم یا اپنے کسی ناجائز کام کے بارے میں بات کرے گا۔ وہ اپنے شکار سے اپنے تعلقات کے حوالے سے غلط بیانی اور جھوٹے وعدے کرتا ہے تاکہ اپنے مقاصد حاصل کر سکے۔

اپنے آپ کو ناپسندیدہ رابطوں سے کیسے بچائیں

اپنے اکاؤنٹس کو پرائیویٹ رکھیں ۔

اپنی پرائیویسی سیٹنگز کا تحفظ کرتے ہوئے آپ اپنے اکاؤنٹ کا جائزہ لے سکتے ہیں کہ آپ کی پوسٹ کون کون دیکھ سکتا ہے اور کون کون آپ سے براہ راست رابطہ کر سکتا ہے۔

روابط ڈیلیٹ کریں

اپنے سوشل میڈیا دوستوں اور فالوورز کی فہرست کا جائزہ لیں ۔ چیک کریں کہ کیا واقعی آپ اس فہرست میں موجود سبھی لوگوں کو جانتے ہیں۔ ایسے رابطوں کو ڈیلیٹ کریں جن کی سرگرمیاں مشکوک نظر آتی ہیں یا ان کی طرف سے کافی عرصے سے کچھ بھی پوسٹ نہیں کیا گیا۔

اسکرین شاٹ کو بطور ثبوت محفوظ رکھیں

ایسے پیغامات، تصاویر، فون نمبر وغیرہ کے اسکرین شاٹس اپنے پاس محفوظ کر لیں جو آپ کے لئے پریشانی کا باعث بن رہے ہوں ۔

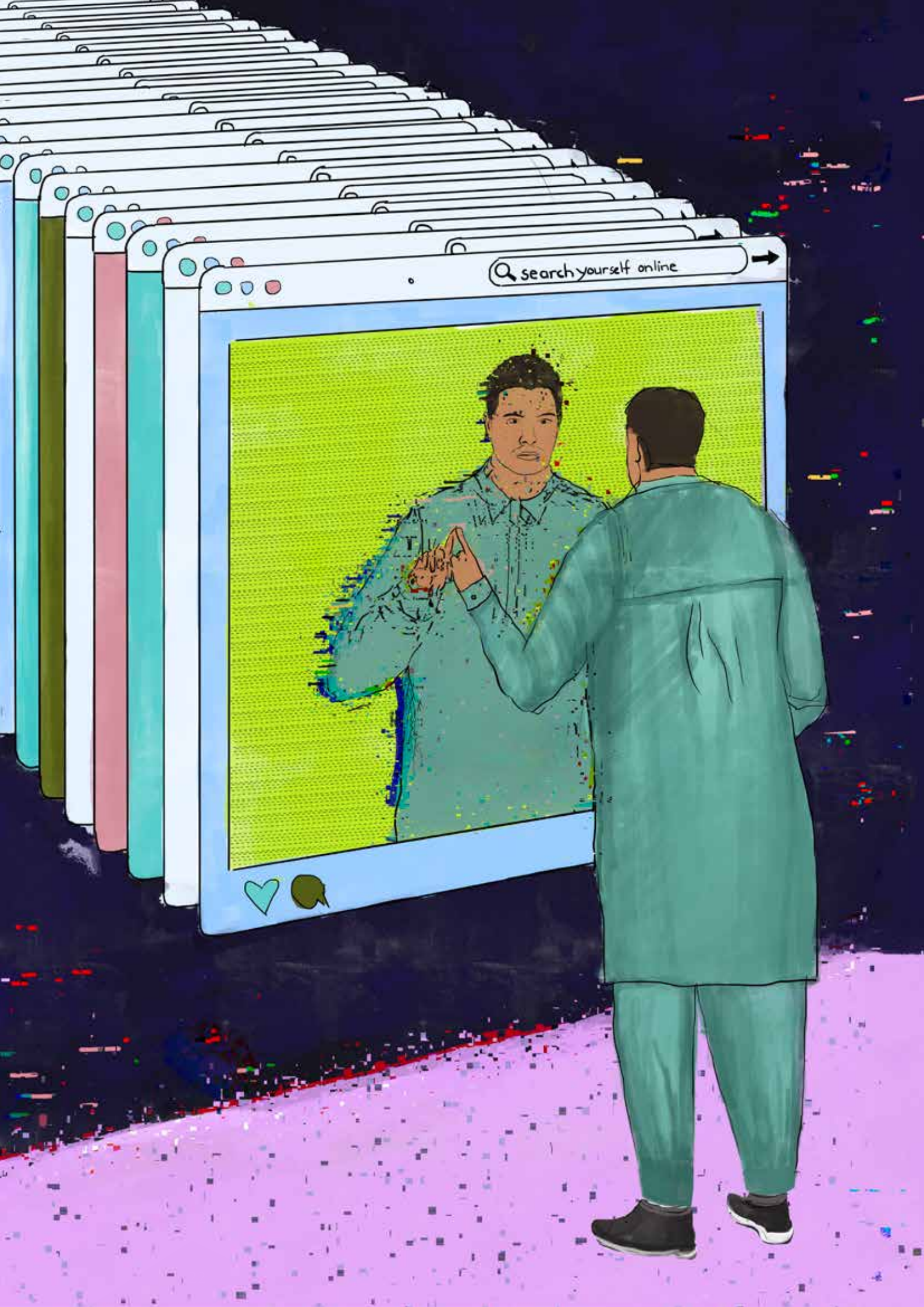
رپورٹ اور بلاک کریں

ایک بار جب آپ کے پاس اپنے تمام اسکرین شاٹس اکٹھے ہو جائیں تو، اس شخص کو براہ راست پلیٹ فارم پر رپورٹ کریں اور پھر اس کا اکاؤنٹ بلاک کر دیں تاکہ وہ آپ کو مزید پریشان کن پیغامات نہ بھیج سکے۔

پولیس کو رپورٹ کریں

سائبر ہراسانی یا بلیک میلنگ کی اطلاع سائبر کرائم ونگ ۔فیڈرل انویسٹی گیشن ایجنسی (ایف آئی اے) کو دیں۔

ہیلپ لائن : 1991
ای میل : helpdesk@nr3c.gov.pk
ویب سائٹ : https://www.fia.gov.pk/ccw


search yourself online

آن لائن شہرت

اچھی شہرت کامیاب زندگی کا پیش خیمہ ثابت ہوسکتی ہے ۔ شاندار ڈیجیٹل شہرت آپ کی کامیابی کے لئے بھی بھرپور مواقع پیدا کرسکتی ہے۔

اپنے آپ کو سرچ کریں
کیا آپ جانتے ہیں کہ آن لائن دنیا آپ کے بارے میں کیا کہتی ہے؟

یہ تشکیل کیسے پاتی ہے؟

مختلف آن لائن سوشل پلیٹ فارمز پر موجود آپ کی پوسٹس اور مواد آپ کی شخصیت کی مکمل عکاس ہیں - کوئی بھی شخص آپ کا نام گوگل میں تلاش کر سکتا ہے یا آپ کے سوشل میڈیا اکاؤنٹس کا جائزہ لے سکتا ہے، جس میں ممکنہ طور پر ملازمت پر رکھنے والے ادارے، یونیورسٹیاں اور دیگر شامل ہیں۔ ایسا مواد جو آپ کی آن لائن ساکھ کی تشکیل کر سکتا ہے اس میں درج ذیل شامل ہیں:-

تصاویر، ویڈیوز، سٹوریز اور رائے جو آپ پوسٹ کرتے ہیں یا دوسروں کے ساتھ شیئر کرتے ہیں۔

آپ کیا پسند اور کیا ناپسند کرتے ہیں۔

وہ لوگ جنہیں آپ آن لائن فالو کرتے ہیں ۔

مثبت ڈیجیٹل فٹ پرنٹ کیا ہے؟

آپ کا ڈیجیٹل فٹ پرنٹ لوگوں کو میسر آن لائن معلومات پر مشتمل ہے۔ یاد رکھیں: انٹرنیٹ پر موجود کوئی بھی مواد کبھی ختم نہیں ہوتا!
آپ اپنے بارے میں جتنی زیادہ معلومات شیئر کریں گے اتنا ہی زیادہ مستقل اور وسیع ریکارڈ آپ کے بارے میں موجود ہوگا۔
مثبت ڈیجیٹل فٹ پرنٹ کے حوالے سے چند رہنما اصول ذیل میں بیان کئے گئے ہیں:-

کوئی بھی مواد پوسٹ کرنے، پسند کرنے یا شیئر کرنے سے پہلے ضرور سوچیں

مثبت ڈیجیٹل موجودگی کی تعمیر کے لئے ضروری ہے کہ آپ کوئی بھی خاص مواد پوسٹ کرنے، لائیک کرنے یا کونٹینٹ کریٹر کو فالو کرنے سے پہلے اپنے آپ سے ضرور پوچھیں کہ کیا آپ واقعی اپنی یونیورسٹی، ممکنہ طور پر ملازمت پر رکھنے والے اداروں، خاندان کے افراد اور دوستوں کو یہ مواد دکھانا چاہتے ہیں ؟

اگر جواب نہیں میں ہے تو مزید پوسٹ کرنے سے پہلے اس بات پر غور کرلیں کہ کہیں یہ مواد بعد میں آپ کے لئے پریشانی کا باعث تو نہیں بنے گا۔

اپنی تخلیقی صلاحیتوں کا اظہار کریں

سوشل میڈیا کا استعمال آپ کی صلاحیتوں اور کامیابیوں کو اُجاگر کرنے کا ایک ذریعہ ہے۔ نوجوان مختلف ویب سائٹس یا اپنے سوشل میڈیا اکاؤنٹس پر اپنے تخلیقی پورٹ فولیو یا کامیابیوں کے مجموعے آن لائن شائع کر سکتے ہیں۔

مثبت مواد تخلیق کریں

تصاویر، پیغامات، ٹوئٹس، ویڈیوز اور سوشل میڈیا پر کوئی بھی تحریری متن آپ کی آن لائن ساکھ قائم کرنے میں اہم کردار ادا کرے گا۔ ایسا مواد ہر گز تخلیق نہ کریں جو جارحانہ ہو اور جس سے کسی خاص مذہب، گروہ یا طبقے کے جذبات کو ٹھیس پہنچے۔

رحمدل بنیں اور سمجھداری کا مظاہرہ کریں

مثبت ڈیجیٹل شہرت کی تعمیر یقینی طور پر محض آن لائن پوسٹ کو لائیک کرنے کی طرح آسان ہے! ایسے کمنٹس کریں جس سے دوسرے کو رہنمائی مل سکے، اور دوست و احباب کے ساتھ زندگی کے مثبت پہلوؤں پر مبنی مواد شیئر کرنے کی تلاش جاری رکھیں۔ اپنی ڈیجیٹل شہرت کا کنٹرول اپنے پاس رکھیں۔

آن لائن منفی شہرت کے نتائج

تعلقات پر اثرات

جارحانہ یا نقصان دہ مواد شیئر کرنے سے آپ کے خاندان اور دوستوں کے ساتھ آپ کے تعلقات پر منفی اثرات مرتب ہو سکتے ہیں ۔ دوسرے لوگ بھی آپ کی شخصیت کے ساتھ نقصان دہ یا نا پسندیدہ مواد منسلک کر سکتے ہیں اور آپ کے ساتھ با مقصد تعلقات کا حصہ نہیں بننا چاہیں گے ۔ جیسا کہ اس کتابچے میں پہلے ہی ذکر کیا گیا ہے، پی ای سی اے 2016 اور پی پی سی کے تحت انٹرنیٹ پر کچھ مواد کی اپ لو ڈنگ اور شیئر نگ غیر قانونی ہے اور آپ قانون کی خلاف ورزی کے مرتکب بھی ہو سکتے ہیں۔

تعلیم اور معاش پر ممکنہ اثرات

ادارے اور بہت سی یونیورسٹیاں اب امیدواروں کو ملازمت یا داخلہ دینے سے پہلے اس کی شخصیت کا جائزہ لینے کے لئے اسے آن لائن سرچ کرتی ہیں۔ کسی ایسی چیز کے بارے میں بات کرنا جس سے آپ متفق نہیں ہیں ایک معقول عمل ہے ۔ تاہم کسی کو نیچا دکھانا، اس کی تضحیک کرنا اور گالی دینا آپ کو نامناسب امیدواروں کی فہرست میں شامل کر سکتا ہے۔

نیٹیکیٹس (انٹرنیٹ کے آداب)

آن لائن شہرت انٹرنیٹ کے آداب کے ساتھ منسلک ہے۔ یہ لفظ ''انٹرنیٹ'' اور ''آداب'' کا امتزاج ہے۔ نیٹیکیٹ آن لائن قابل احترام اور مناسب روابط کے حوالے سے طرز عمل اور اس سے وابستہ قواعد کی وضاحت کرتا ہے۔ اس طرح کے آداب و قواعد کے بغیر آن لائن بات چیت غلط فہمی میں تبدیل ہو سکتی ہے ۔

- **یہ نہ سمجھیں کہ آپ کی بات ہر فرد سمجھ پائے گا۔** درحقیقت انٹرنیٹ مختلف ممالک، ثقافتوں اور نسلوں سے وابستہ افراد کی نمائندگی کرتا ہے۔ اس بات کو مد نظر رکھتے ہوئے گفتگو میں شامل ہونے سے پہلے اپنے کمنٹ کا ایک بار جائزہ ضرور لے لیں۔اپنے آپ سے پوچھیں ''''کیا یہ بات ہر فرد کی سمجھ میں آ پائے گی ؟

- **سپیم نہ بھیجیں** ۔اپنے دوستوں، ساتھیوں اور جاننے والوں کو غیر مطلوبہ ای میلز اور لنکس فارورڈ نہ کریں۔

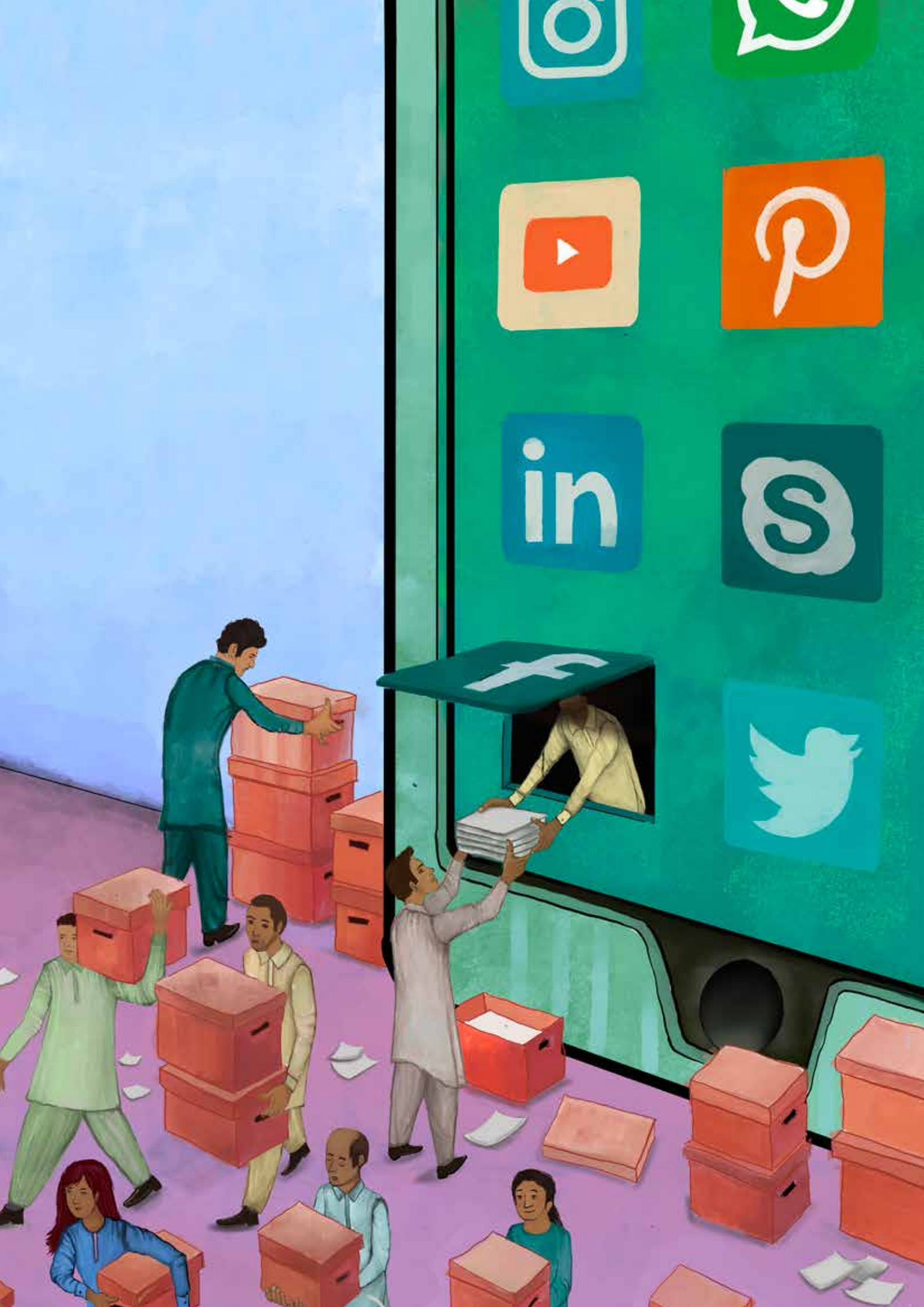
- **درست اور حقیقت پسندانہ رویہ اختیار کریں۔** آپ کے لئے یہ ضروری ہے کہ آپ آن لائن موجود حقائق کی جانچ پڑتال کریں اور مشورہ / معلومات دیتے ہوئے یا کسی پلیٹ فارم یا سائٹ پر شیئر کرتے وقت مواد کے حصول کے ذرائع بھی شامل کریں۔کیوں؟ کیونکہ غلط معلومات عوام الناس کے لئے گمراہ کن اور نقصان دہ ثابت ہو سکتی ہے۔

- **یاد رکھیں، اگر یہ مواد انٹرنیٹ پر موجود ہے، تو اس کا مطلب یہ ہر جگہ دستیاب ہے۔** ایک بار انٹرنیٹ کا حصہ بن جانے والی معلومات ہمیشہ انٹرنیٹ پر دستیاب رہتی ہے۔ یہ ضروری ہے کہ آپ اپنی زندگی کی ہر سرگرمی کی تفصیل آن لائن مہیا نہ کریں بالخصوص کوئی ایسا مواد جو کہ مستقبل میں آپ کے تحفظ کے لئے ایک بڑا خطرہ بن کر آپ کے سامنے آ سکتا ہے۔

- **دوسروں کی رائے کا احترام کریں۔** انٹرنیٹ پر رہتے ہوئے آپ کو چند ایک اختلافات کا بھی سامنا کرنا پڑ سکتا ہے۔ تاہم، آپ کسی کے ساتھ اختلاف رائے بھی کر سکتے ہیں اور ایک ہی وقت میں ان کی رائے کا احترام بھی کر سکتے ہیں۔ لوگوں کے ساتھ اسی طرح کا برتاؤ رکھیں جس کی آپ خود ان سے توقع رکھتے ہیں ۔اس طرح آپ بہت سی ممکنہ پریشانیوں سے بچ جائیں گے ۔

”حقائق کی جانچ پڑتال کریں اور آن لائن پوسٹ کرتے وقت ذرائع ضرور شامل کریں۔“


search yourself online



پرائیویسی اور شناخت کی چوری

آپ کی ذاتی معلومات آپ کا ایک قابل قدر اثاثہ ہے۔
یہ آپ کی ڈیجیٹل اور مالی شناخت پر مشتمل ہے۔

ذاتی طور پر قابل شناخت معلومات (پرسنلی آئی ڈینٹی فائبل انفارمیشن) کیا ہے؟

ذاتی طور پر قابل شناخت معلومات ایسا ڈیٹا ہے جسے کسی کی بھی شناخت کے طور پر استعمال کیا جا سکتا ہے۔ یہ معلومات نام، تاریخ پیدائش، قومی شناختی کارڈ/ پاسپورٹ نمبر، فون نمبر، ای میل ایڈریس اور آئی پی ایڈریسز وغیرہ پر مشتمل ہے۔ اس میں سرچ ہسٹری، تصاویر، خریداری اور لوکیشنز بھی شامل ہیں۔

ڈیٹا کون اکٹھا کرتے ہیں؟

ویب سائٹس، سوشل میڈیا پلیٹ فارمز اور ایپس آپ کے آن لائن طرز عمل پر نظر رکھتی ہیں۔ یہ آپ کی لوکیشن، براؤزنگ کی عادات، ویب ہسٹری کے علاوہ اور بھی بہت سی معلومات اکٹھا کرتی رہتی ہیں۔ یہ ڈیٹا آپ کے بارے میں جیسا کہ آپ کون ہیں، آپ کی گزر بسر، آپ کا سماجی دائرہ کار سمیت آپ کی مکمل زندگی کی تصویر کشی کرتا ہے۔ آپ جن ویب سائٹس کا دورہ کرتے ہیں اور جو ایپس ڈاؤن لوڈ کرتے ہیں وہ ایسا ڈیٹا اکٹھا کرتے رہتے ہیں جو ایڈورٹائزرز کی ضرورت ہوتا ہے تاکہ اس سے باآسانی اندازہ لگایا جا سکے کہ آپ کس قسم کے شخص ہیں اور آپ کو کون سے اشتہارات دکھانے چاہیے۔

آپ سوچتے ہوں گے کہ آپ کے بارے میں آن لائن موجود ڈیٹا کوئی مسئلہ نہیں ہے۔ کیونکہ آپ کے پاس چھپانے کو کچھ بھی نہیں!

آپ جو معلومات آن لائن شیئر کر رہے ہیں: آپ کی ترجیحات، خریداری کی عادات، تعلقات، لوکیشن، مذہبی عقائد، یہاں تک کہ آپ کے اُٹھائے جانے والے ہر ایک قدم پر مشتمل ڈیٹا کاروباری اداروں اور ڈیٹا بروکرز جو آپ کے ڈیٹا سے فائدہ اٹھاتے ہیں کے ذریعہ جمع اور تجزیہ کیا جارہا ہے۔

کس طرح کا ڈیٹا استعمال میں لایا جا سکتا ہے؟

کمپنیاں اپنے مالی مفاد کے لئے فٹنس ٹریکرز سے لے کر گھریلو آٹومیشن ڈیوائسز تک منسلک مصنوعات سے متعلق جمع کردہ ڈیٹا استعمال کرتی ہیں۔ صارفین کو اس حوالے سے آگاہی نہ ہونے کے برابر ہے کہ ان کا ذاتی ڈیٹا کس حد تک اکٹھا کیا جارہا ہے، کون اسے دیکھ رہا ہے اور اس کی اصل قدر و قیمت کیا ہے۔

ڈیٹا بروکرز یا ڈیٹا سروس فراہم کنندگان مختلف ذرائع سے حاصل کردہ صارفین کے ڈیٹا پر مشتمل معلومات کا تجزیہ کرتے ہیں اور اسے فروخت کرتے ہیں۔ یہ معلومات آپ کی زندگی کے ذاتی پہلوؤں جیسا کہ سوشل میڈیا کنیکشنز، سرچ انجن پر کئے گئے سوالات اور آن لائن خریداری وغیرہ پر مشتمل ہے۔ وہ اسے کاروباری اداروں اور سرمایہ کاروں کو فروخت کرتے ہیں جو مختلف کاروباری مقاصد کے تحت اس ڈیٹا سے فائدہ اُٹھاتے ہیں اور اور آمدنی کی نئی راہیں تلاش کرتے ہیں۔ اسی طرح صارف کا ڈیٹا مختلف تعلیمی سرگرمیوں سے وابستہ محققین بھی انسانی رویوں کے مطالعے کے لئے حاصل کرتے ہیں۔

آن لائن پرائیویسی کا تحفظ کیسے یقینی بنائیں؟

اپنی ڈیوائس کا نام تبدیل کریں

ہو سکتا ہے آپ نے اپنے فون، وائی فائی یا بلوٹوتھ کا نام اپنے اصل ''نام'' کے طور پر رکھا ہو جیسا کہ ''احمد کا وائی فائی'' یا یہ دوران سیٹ اپ خود بخود بن گیا ہو۔ اس کا مطلب یہ ہے کہ آپ کے علاقے میں ہر کوئی آپ کا اصل نام دیکھ سکتا ہے۔

اپنی ڈیوائس کی سیٹنگ کے دوران یہ نام ذاتی تعلق سے ہٹ کر کسی کم اہم چیز کی مناسبت سے تبدیل کر لیں۔

اپنی لوکیشن آف رکھیں

آپ کی لوکیشن کے ذریعے آپ اور آپ کے طرز عمل، مثال کے طور پر آپ کی رہائش، جہاں آپ کام کرتے ہیں اور جہاں آپ خاندان اور دوستوں سے ملنا پسند کرتے ہیں سے متعلق اہم تفصیلات افشا ہو سکتی ہیں۔ ہو سکتا ہے کہ آپ نے اپنے فون پر لوکشن بند کر دی ہو لیکن متعدد ایپس پہلے ہی آپ کی نقل و حرکت اور سرگرمیوں کی نگرانی کر رہی ہوں۔

کیوں؟ کیونکہ آپ سے متعلقہ یہ معلومات کمپنیوں اور ڈیٹا بروکرز کے لئے انتہائی قیمتی ہے۔ اپنے فون کی ''سیٹنگ'' پر جائیں اور ہر ایپ کی پرمیشن کا جائزہ لے کر لوکیشن بند (آف) کر دیں (اگرچہ اس ایپ کو آپ کو کسی خدمات کی فراہمی کے لئے آپ کی لوکیشن جاننے کی ضرورت نہیں ہے۔)

اپنے فون میں سے غیر ضروری ایپس کو ختم کر دیں

آپ کے موبائل فون میں ایپس ڈیٹا اکٹھا کرتے رہتے ہیں۔ ایپس سے متعلقہ پرمیشنز کا جائزہ لیں اور اپنا فون باقاعدگی سے چیک کرتے رہیں تاکہ کوئی بھی ایسی ایپ جو آپ کے زیر استعمال نہیں ہے ہٹائی جا سکے۔

پرائیویسی کی اہمیت

موبائل فون اور لیپ ٹاپ میں براؤزر پہلے سے ہی انسٹال ہوتے ہیں جو ہو سکتا ہے کہ آپ کی پرائیویسی کا تحفظ نہ کر سکیں۔ ایک محفوظ براؤزر آپ کے آن لائن تحفظ میں مددگار ثابت ہوتا ہے اور آپ کے ڈیٹا کے غلط استعمال سے آپ کو تحفظ فراہم کرتا ہے۔

اپنی پرائیویسی کے تحفظ اور خود کو غیر ضروری ٹریکنگ سے بچانے کے لئے اپنی ضروریات کے عین مطابق ایک محفوظ براؤزر تلاش کریں۔ مالویئر، اشتہارات اور ٹریکنگ سے تحفظ کے پیش نظر آپ ایڈ آنز اور ایکسٹینشنز ''(add-ons and extensions)'' انسٹال کر سکتے ہیں (یہ آپ کے براؤزر کے لئے چھوٹے آسان مددگار پروگرامز پر مشتمل ہیں جس کے ذریعے آپ اپنی آن لائن سرگرمی کو زیادہ پرائیویٹ بنا سکتے ہیں)۔ ہمیشہ آفیشل ویب اسٹورز سے ایکسٹینشن انسٹال کریں اور اس حوالے سے درکار پرمیشن پر غور کریں۔

ایپ یا ویب سائٹ کس حد تک محفوظ ہے اس بات کی تسلی کر لیں

اس بات کو یقینی بنائیں کہ آپ جو ویب سائٹ دیکھ رہے ہیں اور اس پر اپنا ڈیٹا بھی شیئر کر رہے ہیں آیا وہ مستند بھی ہے کہ نہیں۔ آن لائن تحفظ کے لئے ایک محفوظ ہائپر ٹیکسٹ ٹرانسفر پروٹوکول سیکیور (ایچ ٹی ٹی پی ایس) یو آر ایل اور لاک آئیکن 🔒 تلاش کریں، اور اس بات کو بھی یقینی بنائیں کہ ایڈریس بار میں یو آر ایل کا اندراج درست ہے۔ اگر آپ کا اینٹی وائرس یا براؤزر کسی سائٹ کے دھوکہ دہی میں ملوث ہونے کی نشاندہی کرتا ہے اور آپ کو بہت سے پاپ اپ اشتہارات بھی دکھاتا ہے تو اسے نظر انداز کرنا ہی بہتر ہے! آپ محض آن لائن سرچ کے ذریعے ویب سائٹ یا ایپ کے حوالے سے ریویوز (reviews) کا بھی جائزہ لے سکتے ہیں۔

یاد رکھیں: مشکوک ویب سائٹ یا ایپ کے ذریعے ڈاؤن لوڈ کئے جانے والے سافٹ ویئرز اور پروگرام ممکنہ طور پر پرائیویسی اور تحفظ کے حوالے سے مسائل پیدا کر سکتے ہیں۔ پروگراموں اور ایپس کو ان کے تیار کردہ اور آفیشل ایپ اسٹورز سے ہی براہ راست ڈاؤن لوڈ کریں۔

شناخت کی چوری کیا ہے؟

جب کوئی شخص آپ کی اجازت کے بغیر آپ کی ذاتی یا مالی معلومات کا استعمال کرتا ہے،اسے شناخت کی چوری کہتے ہیں۔ وہ آپ کا نام اور پتہ، کریڈٹ کارڈ، یا بینک اکاؤنٹ نمبر وغیرہ چوری کر سکتے ہیں اور ان کا درج ذیل منفی استعمال کر سکتے ہیں:۔

- بغیر اجازت خریداری/لین دین
- مختلف دھوکہ دہی/مجرمانہ سرگرمیوں میں ملوث

آن لائن شناخت کی چوری کیسے ممکن ہے؟

آن لائن شناخت کی چوری اس وقت ہوتی ہے جب صارفین نقصان دہ ای میل منسلکات کھول لیتے ہیں ،اپنے کمپیوٹرز یا اسمارٹ فونز پر مالوئیر ڈاؤن لوڈ کرتے ہیں یا پھر غیر محفوظ وائرلیس نیٹ ورکس کا استعمال کرتے ہیں اور دوسرے لوگوں کے ساتھ اپنا پاس ورڈ شیئر کرتے ہیں۔

مالویئر اور اسپائی ویئر

مالویئر یا ''خطرناک سافٹ ویئر'' میں وائرس اور اسپائی ویئر شامل ہوتے ہیں جو کمپیوٹر سسٹم میں داخل ہو کر اسے متاثر کر سکتے ہیں۔ صارفین کو پھنسانے کے لئے، مجرم اصل جیسی جعلی ویب سائٹس بناتے ہیں۔ پُرکشش ڈاؤن لوڈز اور اشتہا راتی لنکس کے ذریعے صارفین کو مجبور کرتے ہیں کہ وہ مالویئر ڈاؤن لوڈ کرلیں خاص طور پر ایسے کمپیوٹرز میں جن میں مناسب سکیورٹی سافٹ ویئر موجود نہیں ہے۔

اسپائی ویئر بھی مالوئیر کی ہی ایک قسم ہے جو خفیہ طور پر آپ کے آن لائن طرز عمل کی نگرانی کر سکتا ہے۔ یہ صارفین کو خطرناک ویب سائٹس پر ری ڈائریکٹ کر سکتا ہے، صارفین کو پاپ اپ اشتہارات بھیج سکتا ہے، ان ویب سائٹوں کی نگرانی کر سکتا ہے جن کا صارف وزٹ کرتا ہے یا ذاتی معلومات کی چوری کے لئے ان کے کی اسٹروک (keystrokes) بھی ریکارڈ کر سکتا ہے۔

رینسم ویئر

رینسم ویئر ایک قسم کا مالویئر ہے جو متاثرہ شخص کی فائلوں تک اس قدر رسائی حاصل کرلیتا ہے کہ یہ فائلیں متاثرہ شخص سے خفیہ ہو کر لاک اور انکرپٹ ہو جاتی ہیں ۔ اس کے بعد متاثرہ شخص کو انتباہ جاری کر دیا جاتا ہے کہ ان فائلوں کی واپسی کے لئے تاوان (آن لائن ادائیگی کے طریقوں کے ذریعے) طلب کیا جاتا ہے۔ رینسم ویئر نقصان دہ ای میل منسلکات /لنکس (جسے فشنگ بھی کہا جاتا ہے) یا ڈاؤن لوڈز کا استعمال کرتے ہوئے پھیلایا جاتا ہے۔

آن لائن استحصال کے منصوبے

آن لائن / سائبر استحصال سے مراد طاقت یا دھمکیوں کے ذریعہ سائبر اثاثوں پر قبضہ جمانا یا رقم حاصل کرنا ہے۔ یہ نقصانات مختلف اقسام کے ہو سکتے ہیں لیکن سب سے زیادہ نمایاں نقصانات کی اقسام ذیل میں دی گئیں ہیں:۔

- ذاتی معلومات جیسا کہ نازیبا تصاویر شیئر کر دینا
- کسی شخص یا ان کے پیاروں کو نقصان پہنچانا
- کسی شخص کی شہرت یا اسے مالی طور پر نقصان پہنچانا

جنسی زیادتی (جنسی استحصال)

جنسی زیادتی کے اسکینڈل میں ملوث فرد متاثرہ شخص کی نازیبا تصاویر یا ویڈیوز کو متاثرہ شخص کے دوستوں اوراہل و احباب کو پیسے یا دیگر احسانات کے عوض جاری کرنے کی دھمکی دیتا ہے۔ بلیک میلر کے مطالبات کو تسلیم کرنے کے بجائے کسی قابل اعتماد دوست / خاندان کے افراد کی مدد سے مقامی پولیس کو رپورٹ کریں۔

بذریعہ ای میل استحصال بالجبر

- اس میں متاثرہ شخص کو ای میل کی جاتی ہے اور دعوی کیا جاتا ہے کہ ان کا کمپیوٹر یا ویب کیم ہیک کر کے ان کی ذاتی سرگرمی کو ریکارڈ کر لیا گیا ہے۔
- دھمکی دی جاتی ہے کہ اگر رقم کی ادائیگی نہ کی گئی تو ایسی ریکارڈنگ متاثرہ افراد کی رابطہ فہرست میں موجود تمام افراد کو بھیج دی جائے گی اس میں عموماً کرپٹو کرنسی کا استعمال کیا جاتا ہے۔
- ایک عام حربہ کے طور پر ذاتی ڈیٹا کے قبضے کی اطلاع متاثرہ فرد کو ای میل کے ذریعے دی جاتی ہے ۔ صارف کا اعتماد حاصل کرنے کے لئے پہلے وہ بڑے پیمانے پر ڈیٹا کی خلاف ورزیوں یا ہیکس سے صارف کا ایک سمجھوتہ شدہ اکاؤنٹ پاس ورڈ ظاہر کرتے ہیں۔ اس قسم کی دھوکہ دہی کے ذریعے نابالغ ، بزرگ یا دیگر کمزور افراد کو نشانہ بنایا جاتا ہے۔

شناخت کی چوری سے اپنے آپ کو کیسے محفوظ رکھیں؟

اپنی ذاتی معلومات دینے سے پہلے سوالات پوچھیں

کچھ ادارے آپ کی شناخت کے لئے آپ کے شناختی کارڈ / پاسپورٹ طلب کرتے ہیں۔ ان اداروں میں آپ کا بینک، تعلیمی ادارہ یا جس ادارے میں آپ ملازمت کرتے ہیں بھی شامل ہو سکتا ہے۔

دیگر ادارے جو آپ کے شناختی کارڈ / پاسپورٹ وغیرہ کی معلومات طلب کرتے ہیں ضروری نہیں کہ ان کو ایسی معلومات درکار ہوں۔ لہٰذا اہم ذاتی معلومات دینے سے پہلے ان سے تنقیدی سوالات ضرور پوچھیں:-

- آپ کو اس کی ضرورت کیوں ہے؟
- آپ اس کا تحفظ کیسے کریں گے؟
- کیا آپ شناخت کے لئے کسی اور دستاویز کا استعمال کر سکتے ہیں؟

آن لائن دھوکہ بازوں اور فون پر موجود اپنی معلومات کا تحفظ کریں

آن لائن اکاؤنٹ میں لاگ ان کے لئے ایک مضبوط پاس ورڈ کا استعمال کریں۔ تمام پاس ورڈز محفوظ کرنے کے لئے پاس ورڈ منیجر کا استعمال کریں۔

ملٹی فیکٹر توثیقی عمل لاگو کریں۔

ملٹی فیکٹر توثیقی عمل آپ کو اضافی تحفظ فراہم کرتا ہے جس میں آپ کو اپنے اکاؤنٹ میں لاگ ان کے لئے دو یا دو سے زیادہ تصدیقی طریقہ کار درکار ہوتے ہیں۔ یہ طریقہ کار دو زمروں پر مشتمل ہے جیسا کہ پاس کوڈ یا فنگر پرنٹ کا اسکین یا پھر آپ کا چہرہ۔ دھوکہ بازوں کے لئے ملٹی فیکٹر توثیقی عمل کے ذریعے آپ کے اکاؤنٹس میں لاگ ان کا عمل آپ کا یوزر نام اور پاس ورڈ میسر ہونے کے باوجود بھی مشکل ہو جاتا ہے۔

وشنگ

دھوکہ باز ذاتی/مالی معلومات چرانے کے لیے قابل اعتماد ذرائع کے طور پر اپنے آپ کو ظاہر کرتا ہے۔اس کے لیے وہ آواز پیغامات یا فون کالز کا استعمال کرتا ہے۔

آپ کا ردعمل کیا ہونا چاہیے؟

- مستند ادارے جیسے بینک ، سرکاری ادارے یا ٹی وی چینل کی جانب سے نامعلوم نمبروں سے موصول ہونے والی فون کالوں سے ہوشیار رہیں ۔
- فون پر کبھی بھی ذاتی/مالی تفصیلات کا اشتراک یا تصدیق نہ کریں۔
- متعلقہ سروس فراہم کنندہ کو مشتبہ نمبر کی بلاکنگ کے لئے اطلاع دیں۔

سمشنگ

دھوکہ باز ایس ایم ایس/پیغامات کے ذریعے صارف کی توجہ ٹیکسٹ میسج میں موجود مشکوک اٹیچمنٹ یا لنک کھولنے کی جانب مبذول کراتا ہے ۔

آپ کا ردعمل کیا ہونا چاہیے؟

- مستند ادارے جیسے بینک یا ٹی وی چینل کی جانب سے نامعلوم نمبروں سے موصول ہونے والے ایس ایم ایس سے ہوشیار رہیں ۔
- ہمیشہ ذاتی معلومات فراہم کرنے سے پہلے ذرائع کے قابل اعتبار ہونے کی تسلی کریں ۔
- ایس ایم ایس میں شامل کسی بھی لنک پر کلک نہ کریں نہ ہی اس میں موجود نمبر پر کال کریں۔
- متعلقہ سروس فراہم کنندہ کو نمبر کی بلاکنگ کے لئے اطلاع دیں۔

فشنگ

فشنگ ایک آن لائن حملہ ہے جس میں حملہ آور جعلی ویب سائٹس (جو دیکھنے میں اصل معلوم ہوتی ہے) ، ای میل اور لنکس کا استعمال کرتا ہے تاکہ دوسرا شخص اپنی حساس معلومات جیسا کہ اکاؤنٹ نمبر ، شناختی کارڈ اور پاسورڈ وغیرہ ظاہر کردے ۔

اکثر اوقات ایسی ویب سائٹس اور ای میل میں املاء کی غلطیاں ہوتی ہیں اور ان میں جلد بازی کا عنصر جیسا کہ مقررہ مدت کے اندر انعام/مفت منٹس یا ڈیٹا/موبائل فون وغیرہ حاصل کرنے کا لالچ یا آپ کے اکاؤنٹ کو معطل کرنے کی دھمکی دینا شامل ہوتا ہے۔

آپ کا ردعمل کیا ہونا چاہیے؟

- ہمیشہ ذاتی معلومات فراہم کرنے سے پہلے ذرائع کے قابل اعتبار ہونے کی تسلی کریں ۔
- اگر مشکوک ای میل کسی ایسے شخص کی جانب سے آئی ہے جسے آپ جانتے ہیں تو اس سے کال یا میسج کے ذریعے اس حوالے سے ضرور بات کریں۔
- سرکاری ادارے، بینک یا ٹی وی چینل کبھی بھی آپ سے ای میل کے ذریعے حساس معلومات طلب نہیں کریں گے۔

کریڈٹ/ڈیبٹ کارڈ کی سکمنگ سے آگاہ رہیں

سکمنگ چوری کی ایک قسم ہے جس میں اے ٹی ایم مشین میں ڈیوائس کی تنصیب کے ذریعے آپ کے لین دین کی معلومات محفوظ کر کے چوری کی جاتی ہے ۔ اے ٹی ایم پر اپنے کارڈ کا استعمال کرنے سے پہلے جائزہ لے لیں کہ کہیں کوئی کیمرہ یا پھر ایسی ڈیوائس نصب نہ ہو جس کے ذریعے آپ کا پن کوڈ حاصل کرنے کی کوشش کی جا سکے۔

اپنے لین دین کی جانچ پڑتال کریں

مشکوک سرگرمیوں سے بچاؤ کے لئے باقاعدگی سے بینک اور کارڈ سٹیٹمنٹس کا جائزہ لیں۔ اگر اس میں ایسی ٹرانزیکشنز موجود ہیں جو آپ نے نہیں کی تو فوری طور پر اپنے بینک سے رابطہ کریں۔

شناخت کی چوری کی اطلاع دیں

اگر آپ کو شبہ ہے کہ آپ کی شناخت چوری ہوگئی ہے تو فوری کارروائی عمل میں لائیں۔
شناخت کی چوری کی اطلاع سائبر کرائم ونگ ۔ فیڈرل انویسٹی گیشن ایجنسی (ایف آئی اے) کو دیں

ہیلپ لائن : 1991
ای میل : helpdesk@nr3c.gov.pk
ویب سائٹ : https://www.fia.gov.pk/ccw
سائبر کرائم ونگ آپ سے صورتحال کی تفصیلات معلوم کرے گا۔

پاکستان ٹیلی کمیونیکیشن اتھارٹی

اس گائیڈ تک آن لائن رسائی اور پی ٹی اے کی رہنما ہدایات برائے آن لائن تحفظ سے متعلقہ مزید معلومات کے لئے یہ کوڈ اسکین کریں۔