باب-11

سماج پر اثر (SOCIETAL IMPACT)

5196CH11

میرا خیال ہے کہ کمپیوٹر وائرس کو بھی زندگی سمجھنا چاہیے۔ میرا خیال ہے کہ یہ انسانی فطرت کے بارے میں یہی بتاتا ہے کہ ہم نے اب تک جو زندگی پیدا کی ہے وہ خالصاً تباہ کار ہے۔ ہم نے اپنے خیال ہی میں زندگی کی تخلیق کی ہے۔

— اسٹیفن ہاکنگ
(Stephen Hawking)

11.1 تعارف

حالیہ برسوں میں ڈیجیٹل ٹیکنالوجی کی وجہ سے دنیا جہان میں بڑی تبدیلیاں آئی ہیں۔ اس ٹیکنالوجی نے ہماری زندگی پر غیر معمولی اثرات مرتب کیے ہیں اور بہت سی چیزوں کو زیادہ تیز رفتار، زیادہ آسان اور زیادہ آرام دہ بنا دیا ہے۔ ماضی میں ایک خط کو ہم تک پہنچنے میں کئی کئی دن لگ جاتے تھے اور ہر شخص کے حصے کی کاپی الگ الگ پہنچتی اور وہ الگ الگ جواب دیتا تھا۔ لیکن آج کوئی بھی شخص ایک سے زیادہ اشخاص کو بیک وقت ای میل بھیج سکتا ہے۔ الیکٹرانک ترسیل کی بیک وقت پہنچا دینے کی نوعیت یا صلاحیت نے ہم کو زیادہ اور جلدی کام انجام دینے والا بنا دیا ہے۔

بینک کاری کی صنعت سے ہوابازی تک، صنعتی پیداوار سے ای کامرس تک اشیا اور خدمات کی تحویل اور انجام دہی میں ہم کمپیوٹروں اور ڈیجیٹل ٹیکنالوجی پر ہی منحصر ہیں۔ ڈیجیٹل ٹیکنالوجی کے اطلاقات نے تمام انسانی سرگرمیوں کے دائرۂ کار کو از سر نو متعین بھی کیا ہے اور ان کو ترقی بھی دی ہے۔ آج زیادہ سے زیادہ لوگ تیز رفتار انٹرنیٹ کی مدد سے اسمارٹ فون اور کمپیوٹروں وغیرہ کے ذریعے ڈیجیٹل ٹیکنالوجی کا استعمال کر رہے ہیں۔

ڈیجیٹل ٹیکنالوجی کا پھیلاؤ اتنا کیوں بڑھ گیا ہے؟ اول پی سی یا پرسنل کمپیوٹروں اور انٹرنیٹ کے آنے سے اور پھر اسمارٹ فون کے عام ہونے سے یہ ٹیکنالوجی عام آدمی کی دسترس میں ہے۔

ہم ڈیجیٹل ٹیکنالوجی سے استفادہ کرتے ہیں لیکن ساتھ ہی اس کا غلط استعمال بھی ہو سکتا ہے۔ آیئے معاشرے پر اس ٹیکنالوجی کے اثرات کو بھی دیکھیں اور ان بہترین سرگرمیوں کو بھی نظر میں رکھیں ہمارے لیے ایک محفوظ اور منافع بخش ڈیجیٹل ماحول کی ضامن نہیں۔

11.2 ڈیجیٹل فوٹ پرنٹس (DIGITAL FOOTPRINTS)

کیا آپ نے کبھی آن لائن کچھ معلومات (انفارمیشن) کی تلاش کی ہے؟ کیا آپ نے کبھی آن لائن ٹکٹ کی خریداری کی ہے یا اپنے دوست کے ای میل کا جواب دیا ہے، یا آن لائن کسی کھیل کود کے اسکور کو تلاش کیا ہے؟ ہم جب کبھی اسمارٹ فون، ٹیبلیٹ یا کمپیوٹر وغیرہ کے ذریعے انٹرنیٹ پر معلومات کی تلاش کرتے ہیں تو ہم بہت سی معلومات چھوڑتے رہتے ہیں جن سے ہماری آن لائن سرگرمیوں کا اظہار ہوتا ہے۔ یہی ہمارا ڈیجیٹل فوٹ پرنٹ ہے۔

اس باب میں

سوچیے اور جواب دیجیے

کیا آپ کے ڈیجیٹل فوٹ پرنٹ کا استعمال آپ کے رویوں اور آپ کی اخلاقیات کو سمجھنے میں بھی کیا جاسکتا ہے۔

ہمارے اس ڈیجیٹل فوٹ پرنٹ کی تخلیق ہمارے علم کے بغیر بھی کی جاسکتی ہے اور اس کو استعمال بھی کیا جاسکتا ہے۔ اسی فوٹ پرنٹ میں وہ ویب سائٹ بھی شامل ہیں جن کا ہم وزٹ کرتے ہیں، وہ ای میل بھی ہیں جو ہم بھیجتے ہیں اور ساری معلومات بھی ہوسکتی ہیں جو ہم آن لائن انٹرنیٹ پر ڈال دیتے ہیں۔ اس کے علاوہ کمپیوٹر کا آئی پی ایڈریس، محل وقوع (لوکیشن) اور ڈِوائس سے متعلق خصوصی تفصیلات بھی اس ڈیجیٹل فوٹ پرنٹ میں شامل ہیں۔ یہ ساری معلومات ہدفی اشتہارات کے لیے بھی استعمال کی جاسکتی ہے یا کسی دیگر مقصد کے لیے اس سے سوءِ استفادہ کیا جاسکتا ہے۔ اس طرح جو معلومات ہم چھوڑ رہے ہیں اس کی تفصیل سے آگاہ رہنا بہت اچھا رہتا ہے۔ اس بیداری سے ہم کیا لکھ رہے ہیں، کیا اپ لوڈ کر رہے ہیں، کیا ڈاؤن لوڈ کر رہے ہیں یا آن لائن براؤز (Browse) کر رہے ان سب باتوں کے بارے میں ہم محتاط رہ سکتے ہیں۔

ہم جو ڈیجیٹل فوٹ پرنٹ نیٹ پر چھوڑ جاتے ہیں وہ دو قسم کا ہوتا ہے ایک ایکٹیو ڈیجیٹل فوٹ پرنٹ جس میں وہ ساری معلومات شامل ہے جو ہم ارادتاً آن لائن بتاتے ہیں۔ اس میں ای میل وہ جوابات یا پوسٹ، بھی شامل ہیں، جو ہم مختلف ویب سائٹوں یا موبائل ایپ وغیرہ پر دے دیتے ہیں۔ البتہ وہ ساری ڈیجیٹل معلومات جو ہم بلا کسی قصد اور ارادہ کے آن لائن چھوڑ دیتے ہیں اس کو مجہول (Passive) ڈیجیٹل فوٹ پرنٹس کہا جاتا ہے۔ اس میں وہ معلومات شامل ہوتی ہے جسے ہم کسی ویب سائٹ پر یا کسی موبائل ایپ پر انٹرنیٹ کو براؤز کرتے وقت دیتے ہیں جیسا کہ شکل 11 میں دکھایا گیا ہے۔

ہر وہ شخص جو انٹرنیٹ سے جڑا ہوتا ہے اس کی رسائی اس ڈاٹا تک ہوسکتی ہے۔ زیادہ استعمال سے یہ معلومات اور بڑھ سکتی ہے۔ براؤزر سیٹنگ کی جانچ کرنے پر ہم پتہ لگا سکتے ہیں کہ یہ ہماری براؤزنگ ہسٹری، کوکیز، پاس ورڈس، آٹو فل اور بہت سی دیگر معلومات کو کس طرح ذخیرہ کرتا رہتا ہے۔

براؤزر کے علاوہ ہمارے اکثر ڈیجیٹل فوٹ پرنٹس سرور (Server) میں ذخیرہ ہوتے رہتے ہیں جہاں اپلی کیشن کی میزبانی ہوتی ہے۔ ہوسکتا ہے کہ ہمیں اس ڈیٹا کو حذف کرنے یا محو کرنے کی رسائی نہ ہو اور ہمیں اس ڈیٹا کو استعمال کرنے کے لیے کنٹرول حاصل نہ ہو۔ اسی لیے جب کبھی ڈیٹا کی تفصیل جنریٹ ہوجاتی ہے تو ڈیجیٹل فوٹ پرنٹس باقی رہتے ہیں چاہے ہم بعد میں اپنی آن لائن سرگرمیوں کے بارے میں ڈیٹا کو محو کرنے کی کوشش ہی کیوں نہ کریں۔ اس بات کی کوئی ضمانت نہیں ہوتی کہ انٹرنیٹ سے ہمارے فوٹ پرنٹس مکمل طور پر حذف کر دیے جائیں گے، اسی لیے جب ہم انٹرنیٹ پر ہوں تو ہمیں بہت محتاط ہونے کی ضرورت ہے۔ ہماری ساری آن لائن سرگرمیاں انٹرنیٹ پر بھی اور اس کمپیوٹنگ ڈِوائس پر بھی ہمارے ڈیٹا کے نقوش چھوڑتی ہیں جن کو ہم استعمال کرتے ہیں۔

شکل 11.1: مثالی ویب اطلاقات جو ڈیجیٹل فوٹ پرنٹس پر منتج ہوتے ہیں۔

اس ڈیٹا کو یوزر کا پتہ لگانے، اس کے محل وقوع، ڈوائس اور دیگر تفصیلات کو معلوم کرنے کے لیے استعمال کیا جاسکتا ہے۔

سرگرمی 11.1

ایک ڈیجیٹل شہری ہونے کے ناتے ان مختلف خدمات کی فہرست تیار کیجیے جو آپ کو دستیاب ہیں۔

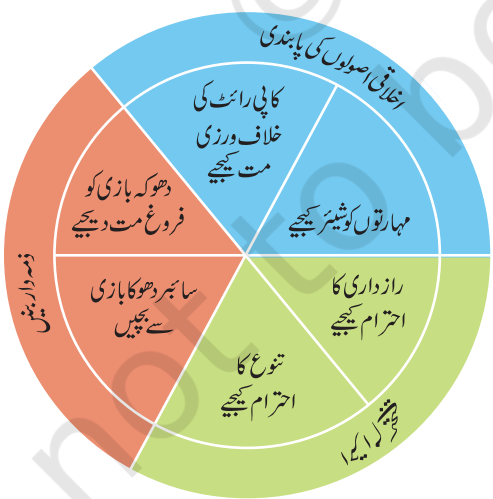
11.3 ڈیجیٹل معاشرہ اور نیٹیزن (DIGITAL SOCIETY AND NETIZEN)

چوں کہ ہمارا سماج زیادہ سے زیادہ ٹیکنالوجی کو استعمال کرنا چاہتا ہے اس لیے اب ہم اپنے زیادہ سے زیادہ کاموں کو ڈیجیٹل طور پر انجام دے کر پورا کر لیتے ہیں۔ ڈیجیٹل معاشرہ کے اس دور میں ہماری روزمرہ کی سرگرمیاں جیسے ترسیل یا ابلاغ، سماجی نیٹ ورکنگ، بینکنگ، خرید وفروخت، تفریحات، تعلیم، نقل وحمل وغیرہ آن لائن مبادلات یا لین دین سے انجام پاتی ہیں۔

اس طرح ڈیجیٹل معاشرہ انسانی سرگرمیوں کے تمام شعبوں میں ڈیجیٹل، ٹیکنالوجی کے استعمال کے بڑھتے رجحان کا مظہر ہے، لیکن آن لائن ہونے کی صورت میں، ہماری سب کی ضرورت ہے کہ ہم اس معاملہ میں بہت محتاط رہیں کہ ہمیں خود کے ساتھ کس طرح پیش آنا ہے اور دوسروں کے ساتھ کس طرح بہتر طریقہ پر ہم برتاؤ کر سکتے ہیں اور ساتھ ہی یہ بھی کہ اپنی اخلاقیات اور اخلاقی اقدار کی کس طرح حفاظت کر سکتے ہیں۔ ہر وہ شخص جو انٹرنیٹ پر ڈیجیٹل ٹیکنالوجیوں کو استعمال کرتا ہے ایک ڈیجیٹل شہری یا نیٹیزن ہے۔ ایک اچھا نیٹیزن ہونے کا مطلب ہے ڈیجیٹل ٹیکنالوجی کا محفوظ، اخلاقی اور قانونی طور پر استعمال کرنا، ایک ذمہ دار نیٹیزن انٹرنیٹ کے آداب، ابلاغ وترسیل کے قوانین اور سماجی میڈیا کے آداب ورسوم کو بجالاتا ہے اور ان کی پابندی کرتا ہے۔

11.3.1 نیٹ کے آداب (Net Etiquettes)

ہم اپنے سماجی تعاملات میں کچھ آداب کی اتباع کرتے ہیں۔ اسی طرح جب ہم آن لائن ہوں تو اس وقت بھی ہم کو کچھ آداب اور کچھ طور طریقوں کا لحاظ رکھنا ضروری ہے۔ (دیکھیے شکل 11.2) اس دوران آن لائن شخص کو جو نیٹ پر سرفنگ کر رہا ہے، اخلاقی اصولوں کا پابند، احترام کرنے والا اور ذمہ داری قبول کرنے والا ہونا چاہیے۔



شکل 11.2: نیٹ کے آداب

(A) اخلاقی اصولوں کی پابندی کیجیے (Be Ethical)

- حق طباعت یا حق اشاعت (Copyright) کی خلاف ورزی نہ ہو۔ اس تمام مواد کو مالک یا تخلیق کار کی اجازت کے بغیر استعمال نہیں کرنا چاہیے جس کے کاپی رائٹ محفوظ ہوں۔ ایک پابند اصول ڈیجیٹل شہری ہونے کے ناتے ویڈیو یا آڈیو کی اسٹریمنگ کے وقت یا تصاویر اور فائلوں کو انٹرنیٹ سے ڈاؤن لوڈ کرتے وقت ہمیں اس موضوع پر کافی معلومات ہونی چاہیے۔ جس معلومات کو سراہا گیا ہے۔ حقیقی اور غیر مبہم ہونی چاہیے۔ اس کے علاوہ، غیر ضروری معلومات سے

احتراز کے لیے ہمیں یہ بھی تصدیق کر لینی چاہیے کہ وہ معلومات پہلے سے انٹرنیٹ پر دستیاب نہیں ہے۔

(B) احترام کیجیے (Be Respectful)

- خلوت (رازداری) کا احترام کیجیے۔ ایک اچھا ڈیجیٹل شہری ہونے کے ناتے ہمیں خلوت (پرائیویسی) اور شخصی اظہار کی آزادی کے حقوق حاصل ہیں۔ ساتھ ہی ساتھ ہمیں یہ بھی سمجھنا ضروری ہے کہ دوسرے ڈیجیٹل شہریوں کو بھی یہی حقوق اور آزادی حاصل ہے۔ کسی ڈیجیٹل شہری کے ساتھ ہماری ترسیل یا ابلاغ میں بھی ایسی تصاویر، دستاویزات وغیرہ شامل ہوسکتی ہیں جو دونوں ہی کے لیے پوشیدگی کے لائق ہوں۔ ہمیں خلوت یا پرائیویسی کے اس حق کا احترام ضروری ہے اور ہم کو یہ تصاویر، دستاویزات اور فائلیں کسی کے بھی ساتھ اس کی مرضی کے بغیر ساجھا نہیں کرنی چاہئیں۔
- تنوع کا احترام کیجیے: کسی گروپ میں یا کی عوامی پلیٹ فارم پر معلومات، تجربات، ثقافت اور دیگر پہلوؤں کے معاملات میں لوگوں کے تنوع یا کثرت کا احترام ضروری ہے۔

(C) ذمہ دار رہیے (Be Responsible)

- سائبر آزار رسانی سے بچیے: کسی کی اہانت، بے عزتی یا آن لائن دھونس دباؤ جیسی افواہوں کو بار بار پوسٹ کرنا، دھمکیاں دینا، کسی شخص کی ذاتی کمیوں کو اجاگر کرنا، جنسی طور پر ہراساں کرنا یا ایسے ریمارکس کسنا جن کا مقصد کسی کا عوامی طور پر مذاق اڑانا وغیرہ کو سائبر آزار رسانی کہا جاتا ہے۔ کسی کو بار بار تکلیف دے کر یا ہراساں کے جان بوجھ کر نشانہ بنانا بھی سائبر آزار رسانی میں شامل ہے۔ ہوسکتا ہے انٹرنیٹ کے نئے یا کبھی کبھی استعمال کرنے والی یوزر یہ محسوس کرتے ہوں کہ آن لائن باتوں کا حقیقی دنیا میں کوئی اثر نہیں ہوتا۔ ہمیں سمجھ لینا چاہیے کہ آن لائن آزار رسانی کے دوسرے لوگوں پر اثرات بہت سنجیدہ نوعیت کے بھی ہوسکتے ہیں۔ اس کے علاوہ یہ بھی یاد رکھیے کہ ہمارے ڈیجیٹل فوٹ پرنٹس کا استعمال کر کے ہماری نیٹ کی معلومات کو دوبارہ واپس لایا جاسکتا ہے۔
- جھگڑوں کو مت بھڑکاؤ: انٹرنیٹ ٹرول وہ شخص ہوتا ہے جو عملاً انٹرنیٹ پر جھگڑے شروع کر کے یا لوگوں میں بے چینی پیدا کر کے، اشتعال انگیز پوسٹ ڈال کے یا کسی آن لائن کمیونٹی کے بارے میں صرف تفریحاً غلط پیغامات بھیج کر تنازعات پیدا کرتا ہوتا ہے۔ چوں کہ ٹرول توجہ کو جلدی اپنی جانب مبذول کر لیتے ہیں اس لیے ان کو اہمیت نہ دینے کا بہت بہتر طریقہ یہ ہے کہ ان سے متعلق تبصروں پر کوئی توجہ نہ دی جائے۔

یاد رکھیے!!

انٹرنیٹ سرفنگ کے وقت ہمیں اپنے ذاتی اور خفیہ ڈاٹا کے بارے میں محتاط ہونا ضروری ہے۔

- ✓ کسی بھی آن لائن پلیٹ فارم پر دوسروں کے ساتھ اپنی ذاتی دستاویزات کی ساجھے داری سے پہلے غور و فکر ضروری ہے۔
- ✓ اپنی ذاتی معلومات کو پاس ورڈس کے ذریعے محفوظ اور صحیح سلامت رکھیے۔

سرگرمی 11.1

پتہ لگائیے کہ کسی دشنام آمیز یا غیر مناسب پوسٹ کے بارے میں یا کسی سوشل نیٹ ورک میں کسی بھیجنے والے کے بارے میں کیسے رپورٹ کریں گے۔

11.3.2 ترسیل کے آداب (Communication Etiquettes)

ڈیجیٹل ترسیل میں ای میل، متن رسانی، فوری پیغامات، سیل فون پر گفتگو، آڈیو یا ویڈیو کانفرنسنگ، انجمنوں سے متعلق پوسٹنگ، سوشل نیٹ ورکنگ سائٹس وغیرہ شامل ہیں۔ خیالات کے تبادل اور معلومات اور علم و دانش کی

سماجی داری کے لیے یہ سب چیزیں لوگوں کو ایک دوسرے سے جوڑنے کے بہترین ذرائع ہیں۔ ای میل پر ابلاغ وترسیل، چیٹ روم اور ایسی ہی دیگر محفلوں میں ایک ڈیجیٹل سٹیزن کو ابلاغ وترسیل کے قوانین یا آداب کی رعایت کرنی ضروری ہوتی ہے۔ شکل 11.3 دیکھیے

شکل 11.3: ترسیل کے آداب

(A) اختصار اختیار کیجیے (Be Precise)

- وقت کا احترام کیجیے: اپنے قیمتی وقت کو غیر ضروری ای میل یا تبصروں کے جواب دینے میں ضائع مت کیجیے جب تک کہ وہ ہمارے لیے کچھ معنویت نہ رکھتے ہوں۔ اسکے علاوہ ہمیں ہمیشہ فوری جواب کی توقع بھی نہیں رکھنی چاہیے کیوں کہ وصول کنندہ کی اور بھی ترجیحات ہوسکتی ہیں۔
- ڈاٹا کی حدود کا بھی احترام کرنا چاہیے۔ ڈاٹا اور بینڈ وڈتھ کے متعلق مسائل کے پیش نظر بہت زیادہ بڑے الحاقات سے پرہیز کرنا چاہیے۔ اس کے برخلاف مختصر اور جامع فائلیں یا ان کے لنک گوگل ڈرائیو، مائکروسافٹ ون ڈرائیو اور یا ہوڈراپ باکس وغیرہ جیسے کلاوڈ شیئر ڈاسٹوریج کے ذریعہ بھیجی جائیں۔

(B) نرم مزاجی اختیار کیجیے (Be Polite)

چاہے ترسیل یا ابلاغ ہم زمان ہو (جیسے بات چیت، آڈیو/ ویڈیو ٹیلیفون گفتگو) یا پھر غیر ہم زمانی ہوں (جیسے ای میل، فورم پوسٹ یا تبصرے) ہمیں اپنی ترسیل میں نرم مزاج ہونا چاہیے اور غیر جارحیت پسند بھی، ہم کسی دوسرے کے نقطہ نظر سے متفق ہوں یا نہ ہوں ہمیں بہرحال بدزبانی سے بچنا ضروری ہے۔

(C) قابل اعتبار رہیے (Be Credible)

جب ہم کسی بات پر تبصرہ یا رائے زنی کریں، کسی بات کا جواب دیں، کسی کو ای میل لکھیں یا پوسٹ ڈالیں تو اس قسم کے سارے امور ایک وقت تک کے لیے ہماری معتبریت کو طے کرتے ہیں۔ اس طرح ہم یہ بھی طے کرتے ہیں کہ فلاں شخص کی فورم پوسٹ کو فالو کرنا ہے اور فورم کے فلاں رکن کو نظر انداز کرنا ہے۔ بحث ومباحثہ کے مختلف فورموں پر ہم عام طور پر کسی بھی شخص کی سابقہ آرا اور نظریات کے ذریعہ ہم ان کی معتبریت کے بارے میں فیصلہ لیتے ہیں اور ان کے تبصروں پر اعتبار کرتے ہیں۔

11.3.3 سوشل میڈیا کے آداب (Social Media Etiquettes)

موجودہ ڈیجیٹل عہد میں ہم مختلف قسم کے سوشل میڈیا سے واقف ہیں اور فیس بک، گوگل +، ٹوئٹر، انسٹاگرام، پنٹریسٹ یا یوٹیوب چینلوں پر ہمارے اکاؤنٹ بھی ہیں۔ سوشل میڈیا ویب سائٹس یا ایپلی کیشن ہیں جو اپنے یوزرس کو کمیونٹی میں مواد کی تخلیق یا دیگر لوگوں کے ساتھ اس کی ساجھے داری کے ذریعہ سوشل نیٹ ورکنگ میں حصہ لینے کے قابل بناتے ہیں۔ یہ پلیٹ فارم تصاویر یا پوسٹوں کے ذریعہ استعمال کنندگان کو اپنے خیالات اور

غیر پسندیدہ ای میل (Spam) سے بچیے!!

ردّی ای میل (جنھیں Spam کہا جاتا ہے) کے ملنے پر نہ تو ان کا جواب دیجیے اور نہ ایسے ای میل کے کسی الحاق کو کھولیے۔

کوئی چیز ہمیشہ کے لیے حذف نہیں ہوتی!!

ہم انٹرنیٹ پر کچھ بھی ڈال سکتے ہیں یا تبصرہ کرسکتے ہیں اور بعد میں اس کو محذوف کرسکتے ہیں۔

✓ لیکن یاد رکھیے کہ یہ چیز ہمیشہ کے لیے حذف نہیں کی جاسکتی۔ یہ چیز ہمارے ڈیجیٹل فوٹ پرنٹس میں باقی رہتی ہیں۔

✓ اسی وجہ سے بہت سے جرائم پسند لوگ جو نفرت پھیلاتے ہیں، دوسروں کو حراساں کرتے ہیں یا دیگر مجرمانہ سرگرمیوں میں ملوث ہوتے ہیں ان کا پتہ لگالیا جاتا ہے اور ان کو گرفتار کرلیا جاتا ہے۔

تجربات کو ساجھا کرنے کی کے لیے شوق دلاتے ہیں۔اس طرح استعمال کنندگان دیگر سوشل میڈیا ایپس اور چینلوں کے آن لائن استعمال کنندگان کے ساتھ خیالات کی ساجھے داری کر سکتے ہیں۔اسی وجہ سے سوشل میڈیا کا اثر اور اس کی ہمہ گیری بہت غیر معمولی طور پر بڑھ گئی ہے۔اس نے سیاست وتجارت، کلچر، تعلیم وغیرہ کے نتائج کی نئی شکل بندی شروع کر دی ہے۔سوشل میڈیا میں بھی کچھ ایسے آداب ہیں جن کی پابندی ہمارے لیے ضروری ہے۔دیکھیے شکل 11.4

حفاظت سے رہیے

- پاس ورڈ کا انتخاب سوجھ بوجھ سے کیجیے۔
- دھیان دیجیے کہ آپ کس کو دوست بنا رہے ہیں۔
- جھوٹی معلومات سے ہوشیار رہیے۔

معتبر رہیے

- اپ لوڈ کرنے سے پہلے غور کر لیجیے۔

شکل 11.4: سوشل میڈیا کے آداب

(A) محفوظ رہیے (Be Secure)

- پاس ورڈ کا انتخاب دانشمندی کے ساتھ کیجیے: یہ بات سوشل نیٹ ورک کے استعمال کنندگان کے لیے بہت ہی اہم ہے۔سوشل نیٹ ورک سے استعمال کنندگان ڈیٹا کی خلاف ورزی یا اس کا انکشاف کبھی کبھی سرخیوں کا موضوع بن جاتا ہے۔استعمال کنندگان کو اس قسم کے امکانات کے متعلق بہت محتاط رہنا چاہیے اور یہ بھی جاننا چاہیے کہ وہ خود کو اور اپنے اکاؤنٹ کو کس طرح محفوظ رکھ سکتے ہیں۔سب سے آسان طریقہ تو یہی ہے کہ پاس ورڈ بھاری بھرکم ہوں اور اکثر وبیشتر تبدیل کر دیے جائیں۔اپنی نجی معلومات مثلاً یوزر نام اور پاس ورڈ میں کسی کو شریک نہ کیا جائے۔
- آپ کس کو دوست بنا رہے ہیں اس کو بھی جاننا ضروری ہے: سوشل نیٹ ورک عام طور پر استعمال کنندگان کے ساتھ رابطوں (دوست بنانے) کو فروغ دیتے ہیں۔کبھی کبھی ہم ان کو بھی دوست بنا لیتے ہیں جن کو ہم جانتے بھی نہیں اور جن سے کبھی ملاقات بھی نہیں ہوتی۔بہرحال ضرورت محتاط رہنے کی ہے خاص طور پر اس وقت جب ہم انجان لوگوں کو دوست بنائیں کیوں کہ ہم کو ان کی بدنیتی معلوم نہیں ہوتی، ہوسکتا ہے وہ ہمارے بدخواہ ہوں اور ان کی دوستی غیر محفوظ ہو۔
- جھوٹی معلومات سے ہوشیار رہیے: غلط خبریں، پیغامات اور پوسٹیں سوشل نیٹ ورکس میں عام ہیں۔ایک استعمال کنندگان کی حیثیت ہمیں ان کے بارے میں احتیاط کی ضرورت ہے۔ہم اپنے تجربات کی بنیاد پر ہم اندازہ لگا سکتے ہیں کہ کون سی خبر، کون سا پیغام یا پوسٹ صحیح ہے اور کون سی غلط۔اس لیے ہمیں آنکھیں بند کر کے کسی ایسی بات پر یقین نہ کریں جو کسی سوشل پلیٹ فارم سے ہمیں دستیاب ہو۔ہمیں اپنا علم، تجربہ اور بصیرت کا بھی استعمال کرنا چاہیے اور ان خبروں، پیغاموں اور پوسٹوں کی صحت کے بارے میں پتہ لگانا چاہیے۔

(B) قابل اعتبار رہیے (Be Reliable)

- اپ لوڈ کرنے سے پہلے خوب سوچ لیجیے: ہم سوشل نیٹ ورک پر ہر چیز اپ لوڈ کر سکتے ہیں۔بہرحال، یہ ضرور یاد رکھیے کہ اپ لوڈ ہو جانے کے بعد وہ ریموٹ سرور میں ہمیشہ باقی رہے گا چاہے ہم فائل کو

ملاقات مت کیجیے!!

- ✓ آن لائن دوست سے ملنے کا اہتمام مت کیجیے ہوسکتا ہے ایسا کرنا محفوظ نہ ہو۔
- ✓ بظاہر آن لائن کوئی شخص بہت معقول لگ رہا ہو لیکن ہوسکتا ہے کہ یہ دھوکا ہو اور اس نے اپنی اصل شناخت کو چھپا رکھا ہو۔

سوچیے اور جواب دیجیے

کیا مختلف ویب سائٹوں پر آپ نے تمام اکاؤنٹ کو ایک ہی پاس ورڈ سے محفوظ کیا ہے؟

محفوظ رہیے

نجی تصاویر کو ساجھا کرنے سے پہلے خوب غور کر لیجیے۔

حذف ہی کیوں نہ کریں۔ اسی لیے اپ لوڈنگ کرتے وقت یا حساس اور خفیہ فائلوں کو بھیجتے وقت ہمیں محتاط رہنا چاہیے جنھیں راز میں رکھنا ہماری ذمہ داری ہے۔

سرگرمی 11.3

فرض کیجیے کسی کا ای میل پاس ورڈ Tecnnology ہے۔ کیا آپ کوئی زیادہ مستحکم پاس ورڈ تجویز کر سکتے ہیں؟

11.4 ڈیٹا کا تحفظ (DATA PROTECTION)

اس ڈیجیٹل دور میں ڈیٹا یا معلومات کے تحفظ کا تعلق خاص طور پر ڈیجیٹل طور پر ذخیرہ شدہ ڈیٹا کی پرائیویسی سے ہے۔ ڈیٹا کے وہ عناصر جو خلاف ورزی یا سمجھوتہ کی صورت میں کسی کے لیے ضرر، ہراس، اضطراب اور ناانصافی کا موجب ہو سکتے ہیں ان کو حساس ڈیٹا کہا جاتا ہے۔ بایومیٹرک معلومات، صحت سے متعلق معلومات، مالی معلومات، دیگر نجی دستاویز، تصاویر، آڈیوز یا ویڈیوز وغیرہ حساس معلومات میں شامل ہیں۔ حساس ڈیٹا کی نجی حیثیت کو رمزی تحریر (Encryption)، تصدیق (Authentication) اور دیگر محفوظ طریقوں سے برقرار رکھا جا سکتا ہے اور یہ یقینی بنایا جا سکتا ہے کہ اس ڈیٹا تک کسی جائز مقصد کے لیے صرف مجاز استعمال کنندہ کی ہی رسائی ہو سکتی ہے۔

سوچیے اور جواب دیجیے

کوئی پروجیکٹ یا کوئی تحریر تار کرنے کے لیے ہم نے کوئی تصور کہاں سے لیا ہے یا ہم نے کن ذرائع (کتاب، تصویر، آڈیو، ویڈیو وغیرہ) کا استعمال کیا ہے۔ اس بارے میں ہمیشہ ہی ان کے ماخذ کا ذکر کیوں ضروری ہے؟

تمام دنیا میں ڈیٹا تحفظ سے متعلق ہر ملک کی اپنی پالیسیاں یا قوانین ہیں۔ یہ پالیسیاں دراصل قانون دستاویزات ہیں جو حساس معلومات کی پروسیسنگ، اسٹوریج اور نشریات کے بارے میں استعمال کنندہ کے لیے رہنما اصول ہیں۔ ان پالیسیوں کے نفاذ کے پس پردہ دراصل مقصد یہ ہے کہ حساس معلومات کسی بھی ترمیم اور انکشاف سے مناسب طریقہ پر محفوظ رہے۔

11.4.1 حقوق روشن فکری (Intellectual Property Right (IPR)

جو کوئی شخص کوئی مکان یا موٹر سائیکل خریدتا ہے تو ہم کہتے ہیں کہ وہ شخص اس جائیداد کا مالک ہے۔ اسی طرح اگر کوئی شخص کوئی نیا تصور لے کر آتا ہے تو یہ تصور یا خیال اس شخص کی فکری یا معنوی ملکیت ہے۔ فکری یا معنوی ملکیت کا تعلق ایجادات یا اختراعات، ادبی یا ہنرمندانہ اظہارات ڈیزائن اور علامت، نام اور لوگو وغیرہ سے ہوتا ہے۔ ان تصورات کی ملکیت کا تعلق اس کے تخلیق کار سے ہوتا ہے یا اس شخص سے ہوتا ہے جو اس فکری یا معنوی ملکیت کا حامل ہے۔ اس سے تخلیق کار یا کاپی رائٹ کے مالک کو اپنی ایجاد یا تخلیق کا استعمال کر کے مالی منفعت یا پہچان بنانے کا حق حاصل ہو جاتا ہے۔ یہ فکری یا معنوی ملکیت کاپی رائٹ، پیٹنٹ اور ٹریڈ مارکس کے ذریعہ قانونی طور پر محفوظ ہوتی ہے۔

(A) حق اشاعت (Data Protection)

حق اشاعت فکری کارناموں جیسے تحریرات، فوٹوگراف، آڈیو ریکارڈنگ، ویڈیو، مجسّموں، تعمیراتی کارناموں، کمپیوٹر سافٹ ویر اور دیگر تخلیقی آثار جیسے ادبی اور آرٹسٹک آثار کے لیے تخلیق کاروں کے قانونی حقوق کو قانونی تحفظ فراہم کرتا ہے۔ تخلیق کاروں اور مصنّفین کو کاپی رائٹس خود حاصل ہو جاتے ہیں۔ کاپی رائٹ قانون کاپی رائٹ کے حامل کو کچھ ایسے حقوق عطا کرتا ہے جس کے نتیجہ میں صرف وہی قانونی طور پر اس کا استعمال کر سکتے

ہیں۔ ان حقوق میں کسی کارنامہ کی نقل (یا اس کی دوبارہ پروڈکشن) کا حق بھی شامل ہے نیز اس پر مبنی کسی اشتقاقی کام (Derivative works) کی تخلیق اس کام کی عام لوگوں کے لیے نقول کی تقسیم، یا اس کام کی عوامی طور پر نمائش یا اس کی اداکاری بھی شامل ہے۔ یہ قانون نقل کرنے یا اس کی فروخت اور اس کو استعمال کرنے سے روکتا ہے۔ مثلاً مصنف رڈیارڈ کپلنگ کے پاس اپنے ناول 'دی جنگل بک' کے کاپی رائٹ محفوظ ہیں، اس کتاب میں جنگل بوائے موگلی کی کہانی بیان کی گئی ہے۔ اگر کوئی شخص اس ناول یا اس کے کسی حصے کو اجازت کے بغیر استعمال کرے گا تو وہ مصنف کے کاپی رائٹ کی خلاف ورزی کا مرتکب ہوگا۔ دوسروں کے کاپی رائٹ کے تحت محفوظ مواد کو استعمال کرے تو اس کو ان سے لائیسنس لینے کی ضرورت ہوگی۔

حقوق روشن فکری پر عمل درآمد: مثلاً کسی سافٹ ویئر کے سلسلے میں

- ✓ کاپی رائٹ کے ذریعہ سافٹ ویئر کے کوڈ کا تحفظ کیا جائے گا۔
- ✓ کسی تصور کے عملی اظہار کا تحفظ پیٹنٹ کے ذریعہ کیا جائے گا۔
- ✓ سافٹ ویئر کا نام اور لوگو/ رجسٹرڈ ٹریڈ مارک کے تحت آتا ہے۔

(B) پیٹنٹ (Patent)

عام طور پر پیٹنٹ ایجادات کے لیے منظور کیا جاتا ہے۔ کاپی رائٹ کے برخلاف ایک موجد کے لیے اپنی ایجاد کو پیٹنٹ کرانے کے درخواست دینی پڑتی ہے۔ جب وہ پیٹنٹ منظور ہوجاتی ہے تو مالک کو دوسرے لوگوں کو اس پیٹنٹ شدہ ایجاد کے استعمال، فروخت اور تقسیم سے روکنے کا خصوصی حق حاصل ہوجاتا ہے۔ اس طرح موجدین دوسرے لوگوں کے ساتھ اپنی سائنسی یا ٹیکنالوجیکل تحقیقات کو ساجھا کرنے کا فائدہ بھی اٹھا سکتے ہیں۔ پیٹنٹ کسی بھی ایجاد کو 20 سال تک تحفظ بخشتا ہے اور اس کے بعد اس کو آزادانہ طور پر استعمال کیا جاسکتا ہے۔ پہچان یا مالی منفعت سے صحیح ماحول کو فروغ ملتا ہے اور مزید حوصلہ افزائی تخلیقیت اور ایجاد و اختراع کے لیے راہ ہموار ہوتی ہے۔

(C) ٹریڈ مارک (Trademark)

ٹریڈ مارکس میں مختلف بصری علامات، لفظ، نام، ڈیزائن، سلوگن (نعرہ) اور لیبل وغیرہ ہوسکتے ہیں جو برانڈ یا کمرشیل کاروبار کو دیگر برانڈس اور کمرشیل دھندوں سے ممتاز کرسکے۔ مثال کے طور پر نائک (Nike) کے سوا کوئی کمپنی جوتے یا کپڑے بیچنے کے لیے نائک برانڈ کا استعمال نہیں کرسکتی۔ اس کے علاوہ دیگر کمپنیاں مبہم قسم کی ملتی جلتی علامات بھی استعمال نہیں کرسکتیں۔ مثلاً دھوکہ میں ڈالنے والے Nikke جیسے برانڈ بھی نہیں استعمال کیے جاسکتے۔ بہرحال غیر متعلق سامان جیسے نوٹ بکس وغیرہ کے نائٹ ٹریڈ مارک کو استعمال کیا جاسکتا ہے۔

11.4.2 روشن فکری ملکیت کے حقوق کی خلاف ورزی (Violation of IPR)

روشن فکری ملکیت کے حقوق کی خلاف ورزی مندرجہ ذیل میں سے کسی ایک طریقہ سے ہوسکتی ہے:

(A) سرقہ (Plagiarism)

انٹرنیٹ کے دستیاب ہونے سے ہم کسی بھی متن تصاویر یا ویڈیو کی نقول حاصل کرسکتے ہیں۔ کسی دوسرے شخص کا آئیڈیا یا اس کی کتاب کو ہم اپنا بنا کر پیش کرسکتے ہیں اس کو سرقہ کہتے ہیں۔ اگر ہم انٹرنیٹ سے کوئی مواد نقل کرتے ہیں لیکن اس کا ماخذ بیان نہیں کرتے یا اس کے اصل تخلیق کار کا نام نہیں لیتے تو اس کو

سرقہ یا چوری کا عمل کہا جائے گا۔ اس کے علاوہ، اگر کوئی شخص کسی خیال یا کسی پروڈکٹ کو پہلے سے موجود خیال یا پروڈکٹ سے اخذ کرتا ہے اور اس کو ایک نیا خیال یا پروڈکٹ بنا کر پیش کرتا ہے تو وہ بھی سرقہ ہی ہوگا۔ یہ ایک بہت سنجیدہ اخلاقی جرم ہے اور کبھی کبھی اس کو فریب دہی مانا جاتا ہے۔ اگر ہم کسی ایسے مواد کو استعمال کریں جس کے استعمال کی اجازت عام ہو تب بھی ہم کو مصنف یا ماخذ کا نام بتانا چاہیے تاکہ سرقے سے بچا جا سکے۔

(B) کاپی رائٹ قانون کی خلاف ورزی (Copyright Infringement)

کاپی رائٹ قانون کی خلاف ورزی اس وقت ہوتی ہے جب ہم کسی دوسرے شخص کے کام کو اس شخص سے اجازت کیے بغیر یا اس کو ادائیگی کیے بغیر استعمال کر لیتے ہیں جب کہ اس کی ادائیگی ضروری ہوتی ہے۔ مان لیجیے ہم انٹرنیٹ سے کسی تصویر کو ڈاؤنڈ لوڈ کرتے ہیں اور اپنے کسی پروجیکٹ میں اس کو استعمال کر لیتے ہیں لیکن اگر اس تصویر کے کاپی رائٹ کا مالک اس کے استعمال کی اجازت نہیں دیتا تو ایسی کسی تصویر کا استعمال خلاف قانون ہوگا چاہے ہم اس کے مصنف اور ماخذ کا نام اپنے پروجیکٹ میں ظاہر بھی کر دیں۔ صرف انٹرنیٹ پر ہونے کی وجہ سے ہم اس کا بلا اجازت استعمال نہیں کر سکتے۔ اس لیے کاپی رائٹ قانون کی خلاف ورزی سے بچنے کے لیے، کسی مواد یا تصویر وغیرہ کے استعمال سے قبل اس کے مصنف یا مالک کی کاپی رائٹ کی صورت حال معلوم کر لی جائے۔

(C) ٹریڈ مارک کی خلاف ورزی (Trademark Infringement)

ٹریڈ مارک کی خلاف ورزی کا مطلب ہے کسی پروڈکٹ یا سروس پر دوسرے کے ٹریڈ مارک کا غیر قانونی استعمال، کسی ٹریڈ مارک کا مالک کسی ایسے شخص کے خلاف قانونی چارہ جوئی کر سکتا ہے جو اس کے رجسٹرڈ ٹریڈ مارک کی خلاف ورزی کرے۔

11.4.3 عمومی رسائی اور اوپن سورس سافٹ ویئر
(Public Access and Open Source Software)

کبھی کبھی کاپی رائٹ سے کسی بھی شخص کے ذریعہ ان کاموں کے استعمال پر پابندی لگ جاتی ہے جن کے کاپی رائٹ محفوظ ہیں۔ اگر دیگر لوگوں کو استعمال کی اجازت ہو اور وہ موجودہ کام کو آگے بڑھائیں تو اس سے مل کر کام کرنے کو بڑھاوا ملے گا اور ایک ہی سمت میں نئی اور اختراعات کو فروغ ملے گا۔ جب پبلک لائسنس کے تحت مصنّفین اپنے کاپی رائٹ شدہ کاموں میں دوسروں کو بھی شامل کر لیں گے تو اس سے دوسروں کو استعمال کرنے اور مزید بہتر بنانے کی بھی اجازت ملے گی۔ اوپن سورس لائسنس سے موجودہ کام یا پروجیکٹ کو کسی شخص کی اجازت کے بغیر موجودہ کام میں اپنا تعاون دینے کا موقع ملے گا۔

GNU جنرل پبلک لائسنس (GPL) اور کری ایٹو کامنس Creative Commons یا CC پبلک لائسنس کے دو مقبول زمرے ہیں۔ ویب سائٹس، موسیقی، فلم، ادبیات وغیرہ جیسے تخلیقی کاموں کی تمام

سرگرمی 11.4

اوپن/ پبلک لائیسنسنگ کے بارے میں معلومات حاصل کرنے کے لیے درج ذیل ویب سائٹ دیکھیے:

(i) creativecommons.org for cc, and
gnu.org for GNU GPL (ii)

ہوشیار!!

- ✓ کسی دوسرے شخص کے کام کو استعمال کرنا اور اس کے استعمال کو مناسب طور پر ظاہر نہ کرنا سرقہ ہے۔
- ✓ کسی دوسرے شخص کے کام کو بغیر اجازت یا بغیر ادائیگی استعمال کرنا (جب کہ اس کی ادائیگی ضروری ہو) کاپی رائٹ کی خلاف ورزی ہے۔

قسموں کے لیے سی سی (CC) کا استعمال کیا جاتا ہے۔ سی سی کے ذریعہ بصورت دیگر کسی کاپی رائٹ شدہ کام کی آزادانہ تقسیم کی اجازت حاصل ہو جاتی ہے اس کا استعمال اس وقت ہوتا ہے جب کوئی مصنف لوگوں کو سا جھا کرنے، استعمال کرنے اور تخلیق شدہ کسی کام پر مزید کام کرنے کی اجازت دیتا ہے۔ بنیادی طور پر کسی سافٹ ویئر کو پبلک لائسنس مہیا کرنے کے لیے GPL کو تیار کیا جاتا ہے۔ GNU GPL ایک دیگر مفت سافٹ ویئر لائسنس ہے جو حتمی استعمال کنندہ (End Users) کو باقاعدہ تازہ معلومات حاصل کرنے کے علاوہ سافٹ ویئر کو چلانے، مطالعہ کرنے، سا جھا کرنے اور اس کی اصلاح کرنے کی آزادی مہیا کرتا ہے۔

استعمال کنندہ ریا کمپنیاں جی پی ایل لائسنس ورکس تقسیم کرتی ہیں وہ نقلوں کی فیس بھی وصول کر سکتی ہیں یا پھر ان کو مفت بھی دے سکتی ہیں۔ یہی چیز GPL لائسنس کو اسکائی ایپ، ایڈوب ایکروبیٹ ریڈر وغیرہ فری ویئر سافٹ ویئر لائسنس سے ممتاز کرتی ہے جو ذاتی استعمال کے لیے تو کاپی کرنے کی اجازت دیتے ہیں لیکن کمرشیل تقسیم یا مالکانہ لائسنس کو ممنوع قرار دیتے ہیں جن میں کاپی رائٹ قانون کے ذریعہ نقل کرنے کی اجازت نہیں ہوتی۔

بہت سے مالکانہ حق والے سافٹ ویئر (Proprietary Software) کمرشیل طور پر فروخت ہوتے ہیں اور ان کے پروگرام کوڈ (سورس کوڈ) کو سا جھا کیا جاتا ہے نہ تقسیم۔ بہر حال کچھ ایسے سافٹ ویئر ہیں جو مفت دستیاب ہیں۔ اور جن کا سورس کوڈ رسائی، اصلاح، تصحیح اور بہتری کے لیے کھلا ہوا ہے۔ فری اور اوپن سورس سافٹ ویئر (FOSS) کے استعمال کنندہ اور ڈویلپرس کا حلقہ بہت بڑا ہے جو نئی خصوصیات یا موجودہ خصوصیات کی اصلاح کا اضافہ کرنے کے لیے مسلسل کوششیں کرتے رہتے ہیں۔ مثلاً Ubuntu اور Fedora جیسے Linux kernel-based آپریٹنگ سسٹم FOSS کے تحت آتے ہیں۔ FOSS کے کچھ مشہور ٹولز (Tools) لبرے آفس (Libre Office) جیسے آفس پیکیجز اور موزیلا فائر فاکس (Mozilla Firefox) جیسے براؤزر وغیرہ ہیں۔

سافٹ ویئر کی چوری سافٹ ویئر کا غیر قانونی استعمال یا تقسیم ہے جو سافٹ ویئر کی کاپی کے لیے لائسنس خریدتے ہیں انھیں کاپی رائٹ مالک کی اجازت کے بغیر اضافی کاپیاں بنانے کا حق نہیں ہے۔ یہ چیز کاپی رائٹ کی خلاف ورزی ہے چاہے اس کا استعمال فروخت کے لیے ہو، مفت تقسیم کے لیے ہو یا خود کاپی کرنے والے کے لیے ہو۔ سافٹ ویئر کی چوری سے ہر شخص کو پرہیز کرنا چاہیے۔ چوری کے سافٹ ویئر کو استعمال کرنا نہ صرف کمپیوٹر سسٹم کی کارکردگی کے لیے ضرر رسانی ہے بلکہ سافٹ ویئر کی صنعت کو بھی اس کا نقصان ہوتا ہے اور نتیجہ کے طور پر ملک کی معیشت پر برا اثر پڑتا ہے۔

یاد رکھیے!!

- ✓ CC لائسنس کاپی رائٹ لائسنس کا ایک مجموعہ یا سیٹ ہے جس سے لائسنس پانے والوں کو تخلیقی مواد نقل کرنے، اس کی اصلاح کرنے اور دوبارہ تقسیم کرنے کے حقوق مل جاتے ہیں لیکن مصنّفین کو لائسنسنگ کی شرائط کے بارے میں فیصلہ کا حق بھی دیتا ہے۔
- ✓ GPL سب سے زیادہ استعمال ہونے والا مفت سافٹ ویئر لائسنس ہے جو اپنے پانے والوں کو نقل کرنے، اصلاح کرنے اور سافٹ ویئر کو دوبارہ تقسیم کرنے کا حق دیتا ہے اور یہی سب حقوق تمام ماخوذ کاموں میں محفوظ ہوتے ہیں۔

11.5 سائبر جرائم (Cyber Crime)

وہ مجرمانہ سرگرمیاں یا جرائم جو ڈیجیٹل ماحول میں انجام دیے جائیں ان کو سائبر جرائم کہا جاتا ہے۔ ایسے جرائم کے معاملہ میں یا تو خود کمپیوٹر نشانہ ہوتا ہے یا کمپیوٹر کو جرم انجام دینے کے لیے بطور ذریعہ استعمال کیا جاتا ہے۔

سائبر جرائم یا تو کسی فرد کے خلاف یا کسی گروہ کے خلاف یا پھر کسی ملک کے خلاف بھی انجام دیے جاتے ہیں۔ اوران کا مقصد براہِ راست بالواسطہ طور پر کسی کو جسمانی تکلیف پہنچانا، مالی نقصان پہنچانا یا ذہنی اور نفسیاتی طور پر ہراساں کرنا ہوتا ہے۔ایک سائبر مجرم کمپیوٹر پر یا دیگر کمپیوٹروں تک پہنچنے کے لیے ایک نیٹ ورک پر حملہ کرتا ہے تا کہ ڈیٹا یا سروسز کو نقصان پہنچا سکے۔اس کے علاوہ، ایک سائبر مجرم بلیک میل کرنے یا رقم اینٹھنے کے مقصد سے پرائیویٹ اور خفیہ معلومات کی چوری کے لیے کمپیوٹر میں وائرس پھیلاتا ہے یا پھر مال ویئر (Malware) ڈال دیتا ہے۔ایک کمپیوٹر وائرس ایک کہنہ جو یا نہ کوڈ کی کچھ ایسی سطریں ہیں جو اپنی ہی نقل کر لیتا ہے اور اس کے کمپیوٹر پر نقصان دہ اثرات مرتب ہوتے ہیں اور یہ سب کام ڈیٹا کو خراب کر کے یا سسٹم کو خراب کر کے انجام دیا جاتا ہے، اسی طرح مالویئر ایک ایسا سافٹ ویئر ہوتا ہے جس کو خصوصی طور پر کمپیوٹر نظام تک غیر مجاز طریقے سے رسائی حاصل کرنے کے لیے تیار کیا جاتا ہے۔ مجرمانہ کارروائیوں کی نوعیت خطرناک حد تک ہر روز بڑھ رہی ہے اور ہر روز ہیکنگ، ٹھگی، خدمات سے انکار، فشنگ (Phishing)، ای میل فراڈ، بینکنگ فراڈ اور شناختی چوری وغیرہ کی رپورٹیں آتی رہتی ہیں۔

یاد رکھیے!!

سائبر جرم ایک ایسا جرم ہے جس میں کمپیوٹر جرم کرنے کا ذریعہ ہوتا ہے۔(ٹھگی، ڈاٹا کی خلاف ورزیاں، چوری وغیرہ)

11.5.1 ہیکنگ (Hacking)

ہیکنگ کمپیوٹر، کمپیوٹر نظام یا کسی بھی ڈیجیٹل سسٹم تک ناجائز طریقے سے رسائی کا عمل ہے، عام طور پر ہیکرز کو ہارڈ ویئر اور سافٹ ویئر کی ٹیکنیکل مہارت حاصل ہوتی ہے۔ وہ کسی سسٹم کو خراب، کرنے یا اس کا غلط استعمال کرنے کے لیے Bugs (خرابیوں/نقائص) وغیرہ کی تلاش میں رہتے ہیں۔

جب ہیکنگ کسی مثبت ارادے سے کی جاتی ہے تو اسے اخلاقی ہیکنگ (Ethical Hacking) کہتے ہیں اور ایسے اخلاقی ہیکرز کو وہائٹ ہیٹ ہیکرس (White Hat Hackers) کہا جاتا ہے۔ یہ لوگ کسی بھی سافٹ ویئر کی ٹیسٹنگ کے دوران کسی کمی یا کمی کے امکان کی تلاش میں رہتے ہیں۔اس طرح کسی سافٹ ویئر کی سلامتی کو بڑھانے یا بہتر بنانے میں مددگار ہوتے ہیں۔ایک اخلاقی ہیکر سکیورٹی کی کمیوں یا کمیوں کے امکانات کا پتہ لگانے کے لیے کسی بھی ویب سائٹ کا استعمال کر سکتے ہیں۔ یہ اخلاقی ہیکر پھر ویب سائٹ کے مالک کو اپنی تحقیقات کے بارے میں رپورٹ دیتا ہے۔اس طرح درحقیقت اخلاقی ہیکنگ سائبر حملوں کے خلاف مالک کو تیار کرتا ہے۔

غیر اخلاقی ہیکر وہ شخص ہے جو حساس ڈیٹا چرانے یا دوسروں کے کمپیوٹر نظاموں کو برباد کرنے کی غرض سے کمپیوٹروں اور کمپیوٹر نظاموں تک ناجائز رسائی حاصل کی کوشش کرتا ہے۔ان کو بلیک ہیٹ ہیکرس (Black Hat Hackers) کہا جاتا ہے۔ان کی اہم وجہ سکیورٹی کو توڑنے اور ڈیٹا کی چوری پر مرکوز ہوتی ہے۔ یہ لوگ ناجائز اور غلط مقاصد کے لیے اپنی مہارتوں کا استعمال کرتے ہیں۔ایسے ہیکرز شناخت کی چوری، مالی منفعت، کسی سابقہ کار یا رقیب گروپ کی سائٹ کو بیکار کرنے یا حساس معلومات کو فاش کرنے کے لیے سکیورٹی نظاموں کو توڑنے کی کوشش کرتے ہیں۔

سرگرمی 11.5

آپ کسی میل گروپ سے اپنا سبسکرپشن کس طرح رد (Unsubsribe) کر سکتے ہیں یا کسی ای میل بھیجنے والے کو کس طرح بلاک کر سکتے ہیں۔

11.5.2 فشنگ اور فراڈ ای میل (Phisingh and Fraud Emails)

فشنگ ایک غیر قانونی سرگرمی ہے۔ اس میں دھوکہ دے کر حساس اور ذاتی معلومات حاصل کرنے کے لیے استعمال کنندہ کے سامنے ایسی جھوٹی (Fake) ویب سائٹیں یا ای میل پیش کیے جاتے ہیں جو بظاہر اصل اور معتبر لگتے ہیں۔ ذاتی معلومات میں استعمال کنندہ کا نام، پاس ورڈ بینکنگ اور کریڈٹ کارڈ کی تفصیل شامل ہے۔ فشنگ کا سب سے عام طریقہ ای میل کی نقل (Spoofing) ہے۔ اس میں ایک نقلی ای-میل ایڈریس کا استعمال کیا جاتا ہے اور یوزر سمجھتا ہے کہ یہ معتبر ذریعہ یا ماخذ ہے۔ اس طرح آپ کو کسی ایسے پتہ (ایڈریس) سے ای میل مل سکتا ہے جو آپ کے بینک یا تعلیمی ادارے جیسا ہو اور جس میں آپ سے معلومات طلب کی گئی ہو لیکن اگر آپ غور سے دیکھیں تو آپ کو پتہ چلے گا کہ ان کا URL ایڈریس غلط ہے۔ یہ لوگ اکثر اصل جیسا لوگو استعمال کرتے ہیں جس کی وجہ سے اصلی نقلی میں پہچان مشکل ہو جاتی ہے۔ فشنگ اکثر فون کال سے یا پھر تحریری پیغامات کے ذریعے سے ہوتی ہے اور آج کل یہ طریقہ بہت عام ہے۔

ہوشیار!!

ناقابل اعتماد ای میل سے لنک قبول کرنا خطرناک ہوسکتا ہے کیوں کہ ممکن ہے یہ وائرس ہوں یا وہ لنک ناقابل اعتماد ویب سائٹوں سے جڑے ہوسکتے ہیں۔ ہم کسی ای میل لنک یا ملحقہ کو اسی وقت کھولیں جب وہ کسی قابل اعتماد ذریعہ سے آیا ہو اور مشکوک نہ ہو۔

(A) سارقین شناخت (Identity Theft)

سارقین شناخت یا شناخت کی چوری کرنے والے کمپیوٹروں یا کمپیوٹری نظاموں سے چوری شدہ ذاتی معلومات (ڈیٹا) کو استعمال کرتے ہیں اور اس غیر قانونی طور پر حاصل شدہ مواد کو استعمال کر کے دھوکہ دھڑی کرتے ہیں۔ کسی استعمال کنندہ کا قابل شناخت ذاتی ڈایا جیسے آبادیاتی تفصیلات، ای میل آئی ڈی، بینکنگ تفصیل، پاسپورٹ، پین، آدھار نمبر اور مختلف ذاتی ڈاٹا کو ہیکر چرا لیتے ہیں اور مالک کی طرف سے اس کا غلط استعمال کیا جاتا ہے۔ یہ فشنگ حملوں کا ایک طریقہ ہے جس کا خاص مقصد مالی منفعت ہے۔ فشنگ کے اور بھی بہت سے طریقے ہوسکتے ہیں جن کے ذریعہ جرائم پسند لوگ کسی شخص کی آئی ڈی چرا کر فائدہ اٹھاتے ہیں۔ ذیل میں کچھ مثالیں دی جاتی ہیں:

- فنانشیل آئی ڈی کی چوری: مالی مقصد کے حصول کے لیے چوری کی آئی ڈی استعمال کی جاتی ہے۔
- اپنی اصل آئی ڈی کا پتہ نہ چلے اس کے لیے جرائم پسند چوری کی آئی ڈی استعمال کرتے ہیں۔
- میڈیکل آئی ڈی کی چوری: جرائم پسند چوری کی آئی ڈی کا استعمال میڈیکل ڈرگس یا علاج کے لیے کرتے ہیں۔

11.5.3 تاوان (Ransomware)

یہ سائبر جرائم کی ایک الگ قسم ہے۔ اس میں حملہ آور کمپیوٹر تک رسائی حاصل کر کے استعمال کنندہ کی کمپیوٹر تک رسائی کو بلاک کر دیتا ہے۔ عام طور پر ایسا ڈاٹا کے اینکرپشن (Encryption) کے ذریعہ کیا جاتا ہے۔ حملہ آور اپنے شکار کو بلیک میل کر کے اس کو ڈاٹا تک رسائی حاصل کرنے کے لیے کچھ رقم کی ادائیگی کے لیے کہتا ہے یا کبھی کبھی اس کے ذاتی اور حساس ڈیٹا یا فوٹو کو چھاپ دینے کی دھمکی دیتے ہیں ورنہ تاوان کی رقم ادا کی جائے۔

رینسم ویئر (Ransomware) کو اس وقت ڈاؤن لوڈ کیا جاتا ہے۔ جب استعمال کنندہ کسی برے مقصد سے یا غیر محفوظ ویب سائٹ کو استعمال کر رہا ہو یا مشکوک مخزن سے کسی سافٹ ویئر کو ڈاؤن لوڈ کر رہا ہو۔ کچھ رینسم ویئر اسپام میل یا غیر مطلوب میل میں ای میل اٹیچ مینٹ کے طور پر بھیج دیے جاتے ہیں۔ یہ ہمارے سسٹم میں بھی اس وقت پہنچ جاتے ہیں جب ہم انٹرنیٹ پر بدنیتی پر مبنی کسی اشتہار پر کلک کر دیتے ہیں۔

سرگرمی 11.6

پتہ لگائیے کہ آپ کے علاقے میں سائبر سیل (Cell) پر شکایت کس طرح درج کرائی جائے گی۔

11.5.4 سائبر جرائم کی روک تھام اور اس کا مقابلہ
(Combatting and Preventing Cyber Crime)

سائبر جرائم کے چیلنجوں کا مقابلہ یا روک تھام کرنے کے لیے ہوشیاری کی بھی ضرورت ہے اور قانونی مدد کی بھی ضرورت ہے۔ سائبر جرائم کے خطرے کو کم کرنے کے لیے مندرجہ ذیل امور کو دھیان میں رکھنا ضروری ہے:

- اہم معلومات یا ڈاٹا کی باقاعدہ جانچ اور دیکھ بھال کیجیے۔
- اینٹی وائرس سافٹ ویئر کا استعمال کیجیے اور اس کو ہمیشہ یا اپ ڈیٹ رکھیے۔
- مسروقہ سافٹ ویئر کو انسٹال کرنے سے پرہیز کیجیے۔ ہمیشہ جانی مالی اور محفوظ سائٹوں (HTTPS) سے سافٹ ویئر ڈاؤن لوڈ کیجیے۔
- سسٹم سافٹ ویئر کو ہمیشہ اپ ڈیٹ تازہ رکھیے۔ اس میں انٹرنیٹ کے براؤزر اور دیگر اپلی کیشن سافٹ ویئر وغیرہ شامل ہیں۔
- ناقابل اعتبار ویب سائٹوں کا استعمال مت کیجیے اور نہ ان سے ڈاؤن لوڈ کیجیے۔
- عام طور پر براؤزر ان مشکوک ویب سائٹ کے بارے میں استعمال کنندہ کو متنبہ کرتا رہتا ہے جن کے تحفظی سرٹیفکیٹ کی تصدیق نہیں کی جاسکتی ہے۔ ایسی ویب سائٹوں سے پرہیز کیجیے۔
- ویب لاگنگ کے قوی پاس ورڈ کا استعمال کیجیے اور وقفہ وقفہ سے اس کو تبدیل کرتے رہیے۔ تمام ویب سائٹوں کے لیے ایک ہی پاس ورڈ کا استعمال مت کیجیے۔ اعداد اور دیگر علامتوں یا حروف وغیرہ کے مختلف پاس ورڈ استعمال کیجیے۔ اپنے پاس ورڈس میں عام الفاظ مت استعمال کیجیے۔
- کسی دیگر شخص کے کمپیوٹر کا استعمال کرتے وقت براؤزر کو یہ اجازت مت دیجیے کہ وہ پاس ورڈ یا آٹوفل ڈاٹا کو محفوظ (Save) کرلے اور اپنے پرائیویٹ براؤزر ونڈو میں براؤز کرنے کی کوشش کیجیے۔
- کسی نامعلوم سائٹ کے لیے اگر آپ سے کہا جائے تو Yes یا No متبادل کے ذریعہ کوکیز (Cookies) کے استعمال پر راضی نہ ہوں۔
- شاپنگ، ٹکٹنگ اور ایسی ہی دوسری خدمات کے لیے آن لائن لین دین صرف مشہور اور محفوظ ویب سائٹوں سے کیجیے۔
- گھر پر ہمیشہ وایرلیس نیٹ ورک کو قوی پاس ورڈ سے محفوظ رکھیے اور اس کو بدلتے رہیے۔

11.6 انڈین انفارمیشن ٹیکنالوجی ایکٹ (INDIAN INFORMATION TECHNOLOGY ACT : IIT ACT)

انٹرنیٹ کی ترقی کے ساتھ ساتھ بہت سے سائبر جرائم — فراڈ، سائبر حملے اور سائبر دھوکہ بازی — کے واقعات بھی بڑھتے ہیں۔ دھوکہ دھڑی کی سرگرمیوں اور جرائم کی نوعیت تبدیل ہوتی رہتی ہے۔ ان خطرات سے مقابلہ کے لیے بہت سے ملکوں نے اپنے ذاتی اور حساس ڈیٹا نیز انٹرنیٹ استعمال کنندگان کے حقوق کے تحفظ کے لیے اقدامات کیے ہیں۔ ہندوستانی حکومت کے انڈین انفارمیشن ٹیکنالوجی ایکٹ 2000 (جسے IT Act بھی کہا جاتا ہے) کے اندر 2008 میں ترمیم کی گئی۔ اس میں تمام فریق کار کے بارے میں اور حساس معلومات کے ذخیرہ اور اس کی ترسیل کے بارے میں رہنما اصول تیار کیے ہیں۔ بہت سی ہندوستانی ریاستوں میں پولس اسٹیشنوں پر سائبر سیل بھی موجود ہیں جہاں کسی بھی سائبر جرم کے خلاف رپورٹ درج کرائی جاسکتی ہے۔ اس قانون میں الیکٹرانک ریکارڈ اور ڈیجیٹل دستخطوں کو منظوری دے کر الیکٹرانک حکمرانی کے لیے قانونی فریم ورک مہیا کیا گیا ہے اور اس قانون کے تحت سائبر جرائم اور ان کے لیے سزاؤں کا ایک خاکہ بھی تیار کیا گیا ہے۔

سائبر جرائم جیسے کمپیوٹر ماخذی دستاویزات سے چھیڑ چھاڑ، کمپیوٹر نظام کو ہیک کرنا، کسی کی ذاتی حساس معلومات کی بنا اجازت اشاعت وغیرہ سے پیدا ہونے والے جھگڑوں کو حل کرنے کے لیے ایک سائبر اپیل ٹری بیونل قائم کیا گیا ہے۔ اس قانون کی ضرورت اس لیے ہے کہ لوگ انٹرنیٹ پر کریڈٹ کارڈس کے ذریعہ غلط استعمال کے خوف کے بغیر لین دین کرسکیں۔ نہ صرف لوگ بلکہ قانون سرکاری اداروں کو بھی ڈیجیٹل فارمیٹ میں سرکاری دستاویزات کی تخلیق اور ان کی اسٹوریج نیز ان کی فائلنگ کو قبول کرنے کا حق عطا کرتا ہے۔

11.7 صحت پر اثرات (IMPACT ON HEALTH)

چوں کہ ڈیجیٹل ٹیکنالوجی مختلف شعبوں میں داخل ہوچکی ہے چنانچہ ہم اسکرین کے سامنے زیادہ وقت بتانے لگے ہیں خواہ وہ موبائل ہو، لیپ ٹاپ، ڈیسک ٹاپ، گیمنگ کنسول، موسیقی یا صوتی آلات ہوں۔ لیکن ایک غیر مناسب وضع اختیار کرکے ہمارے لیے جسمانی اور ذہنی دونوں طرح سے مضر ثابت ہوسکتا ہے۔ علاوہ ازیں، انٹرنیٹ پر بہت زیادہ وقت گزارنا ہمارے لیے معدی ثابت ہوسکتا ہے نتیجتاً ہماری جسمانی و نفسیاتی صحت پر منفی اثرات مرتب ہوسکتے ہیں۔

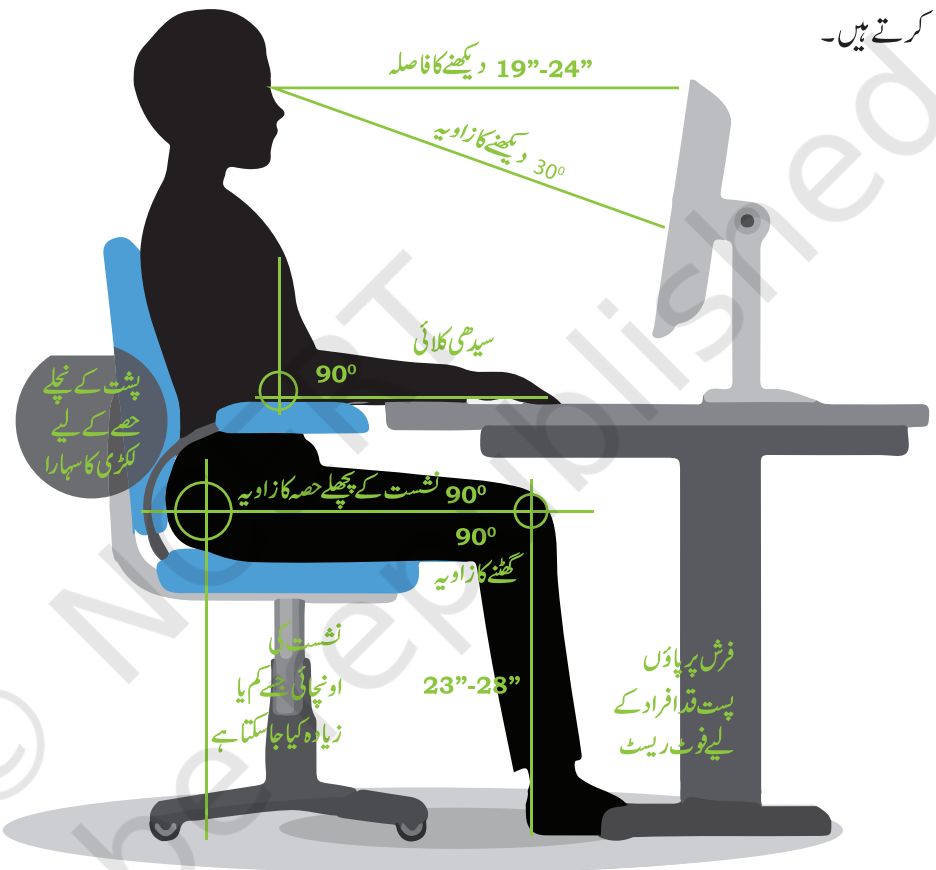
حالاں کہ ہم ان آلات کو جس حالت (یا انداز) میں رکھتے ہیں اسے اور اپنی جسمانی وضع کو درست کرکے صحت سے متعلق ان تشویشات کو کچھ حد تک کم کرسکتے ہیں۔ ارگونومکس (Ergonomics) سائنس کی وہ شاخ ہے جو فرنیچر، آلات اور سسٹم سمیت ورک پلیس کو ڈیزائن یا منظّم کرنے سے متعلق ہے تاکہ یہ استعمال کنندہ کے لیے محفوظ اور آرام دہ بن جائے۔ ارگونومکس ہمارے جسم پر پڑنے والے تناؤ کو کم کرنے میں مدد کرتی ہے

آلہ کی حفاظت: کمپیوٹر سسٹم کی اچھی صحت کی ضامن ہے۔

- ✓ گرد و غبار کو دور رکھنے کے لیے اسے باقاعدگی سے صاف کرتے رہیں۔ الیکٹرانک اسکرین کو صاف کرنے کے لیے خاص طور سے تیار کیے گئے رقیق محلول کا استعمال کریں۔
- ✓ مانیٹر اسکرین کو باقاعدہ طور پر مائکرو فائبر نرم کپڑے (جسے عینک کے شیشوں کو صاف کرنے کے لیے استعمال کیا جاتا ہے) سے صاف کریں۔
- ✓ اسے براہ راست گرمی یا دھوپ سے بچائیں اور ایسے کمرے میں رکھیں جہاں ہوا کے آنے جانے کا مناسب انتظام ہو۔
- ✓ کی بورڈ پر کھانے پینے کی چیزیں نہ رکھیں۔ اگر کھانے پینے کی چیزیں کلید کے درمیان کی جگہ میں گر جاتی ہیں تو آلات کے لیے مسائل پیدا ہوسکتے ہیں۔

جس میں طویل مدتی استعمال کی وجہ سے ہونے والی تکان اور چوٹ شامل ہیں۔

جب ہم کوئی ویڈیو دیکھنے، ٹائپنگ، چیٹنگ یا گیم کھیلنے وغیرہ کے دوران مسلسل طور پر اسکرین کو دیکھتے ہیں تو ہماری آنکھیں اسکرین سے آنے والی چمک کا مسلسل سامنا کرتی ہیں ۔ چھوٹی جسامت کے دستی آلات (handheld devices) کو دیکھنے سے صورت حال اور بھی خراب ہوسکتی ہے۔ آنکھوں میں کھنچاؤ یا تناؤ ایک ایسی علامت ہے جس کی شکایت ڈیجیٹل ڈیوائسز کو استعمال کرنے والے افراد عام طور سے کرتے ہیں۔



شکل 11.5 : کمپیوٹر کے سامنے بیٹھنے کی درست جسمانی وضع

دیکھنے کا فاصلہ اور زاویہ کے ساتھ ساتھ پوزیشن کو اگر ارگونومی کے مطابق ترتیب دیا جائے تو کافی مدد مل سکتی ہے۔ شکل 11.5 میں یہ دکھایا گیا ہے کہ کمپیوٹر سسٹم اور دیگر ڈیجیٹل ڈیوائسز کو زیادہ دیر تک استعمال کرنے کی وجہ سے ہونے والی تکان سے بچنے کے لیے ہمیں کس قسم کی جسمانی وضع اختیار کرنی چاہیے۔ حالاں کہ آنکھوں کے خشک ہوجانے یا ان سے پانی بہنے یا خارش سے بچنے کے لیے وقتاً فوقتاً دور واقع چیزوں پر نظر جمانا اور کام سے فراغت حاصل کرکے بیرونی سرگرمیوں میں شرکت کرنا مفید ثابت ہوتا ہے۔

اگر ورک پلیس کا بندوبست ارگونومکس کی تجاویز کے مطابق کیا جائے تو غیر مناسب وضع، پیٹھ درد، کاندھے اور گردن کے درد سے نجات مل سکتی ہے۔ ایسے کی بورڈ (خواہ وہ مادی کی بورڈ ہو، ٹچ کی بورڈ یا ورچول کی بورڈ ہو) کا کثرت سے استعمال جسے ارگونومی کے مطابق ترتیب نہیں دیا گیا ہے۔ کلائی اور انگلیوں میں درد کا سبب بن سکتا

نوٹ

ہے اور اگر یہ صورت حال لمبے عرصے تک برقرار رہے تو طبی مدد کی ضرورت پڑ سکتی ہے۔

تناؤ، جسمانی تکان، موٹاپا اسی سے متعلق دیگر اثرات ہیں جو ڈیجیٹل ڈیوائسز کو بہت زیادہ دیر تک استعمال کرنے کی صورت میں ہمارے جسم پر مرتب ہو سکتے ہیں۔

خلاصہ

- ڈیجیٹل فوٹ پرنٹ ڈیٹا کے وہ نشانات ہیں جنھیں ہم کسی ویب سائٹ (یا کسی آن لائن اپلی کیشن یا پورٹل کا استعمال کرتے ہیں) پر ڈیٹا کو درج کرنے یا کوئی ٹرانزیکشن (لین دین) کرنے کے دوران پیچھے چھوڑ دیتے ہیں۔
- ڈیجیٹل ٹیکنالوجی کے استعمال کنندہ کو انٹرنیٹ سے متعلق آداب و اطوار، ترسیل سے متعلق آداب واطوار اور سوشل میڈیا سے متعلق آداب واطوار کا پابند ہونا ضروری ہے۔
- نیٹ کے آداب (Net-etiquette) میں مہارتوں کو سمجھا کرنے کے علاوہ حق اشاعت کی خلاف ورزی سے گریز کرنا، استعمال کنندگان کی خلوت (اخفائے راز) اور تنوع کا احترام، سائبر آزاررسانی (Cyber trolls)، سائبر ہراسانی (Cyber bullies) سے گریز کرنا شامل ہے۔
- ترسیل سے متعلق آداب گفتگو کے دوران نرم مزاجی اختیار کرنے اور درست گوئی کے متقاضی ہیں تاکہ اپنے تبصروں اور رائے زنی کے تعلق سے ہماری معتربیت قائم رہے۔
- سوشل میڈیا کا استعمال کرتے وقت پاس ورڈ کی مدد سے تحفظ وسلامتی کا خیال رکھنا چاہیے۔ جھوٹی اور غلط معلومات سے خبردار رہنا چاہیے اور نا آشنا لوگوں سے دوستی کرتے وقت محتاط رہنے کی ضرورت ہے۔ سوشل میڈیا پر کچھ بھی سمجھا (شیئر) کرتے وقت بہت زیادہ احتیاط برتنے کی ضرورت ہے کیوں کہ اگر خاص طور سے ہماری نجی، حساس معلومات کو غلط طریقے سے استعمال کیا جائے تو اس سے بدامنی پیدا ہو سکتی ہے۔
- حقوق روشن فکری (IPR) کاپی رائٹ، پیٹنٹ اور ٹریڈ مارک کے ذریعے سے ڈیٹا کے تحفظ میں مدد کرتے ہیں۔ IRP کی خلاف ورزی کے اخلاقی اور قانونی دونوں پہلو ہیں۔ ایک اچھے ڈیجیٹل شہری کو ادبی سرقہ، کاپی رائٹ کی خلاف ورزی اور ٹریڈ مارک کی خلاف ورزی سے گریز کرنا چاہیے۔
- کچھ سافٹ ویئر مفت عوامی رسائی کے لیے دست یاب ہیں۔ مفت اوپن سورس سافٹ ویئر (FOSS) ایسے سافٹ ویئر ہیں جنھیں استعمال کنندہ نہ صرف ایکسس کر سکتے ہیں بلکہ ان میں ترمیم (اصلاح) کر سکتے ہیں۔

نوٹ

- سائبر جرائم میں ڈیٹا کی چوری یا اہم خدمات میں رخنہ پیدا کرنے کے لیے انجام دی جانے والی مجرمانہ سرگرمیاں شامل ہیں۔ان سرگرمیوں میں ہیکنگ، وائرس یا مالویئر (Malware) پھیلانا، فشنگ، دھوکہ دہی والے ای میل بھیجنا، رینسم ویئر (Ransomware)، وغیرہ شامل ہیں۔
- ڈیجیٹل آلات کے بہت زیادہ استعمال سے ہماری جسمانی ونفسیاتی صحت پر منفی اثرات مرتب ہوسکتے ہیں۔آلات کی ارگونومک ترتیب کے ساتھ ساتھ ہماری جسمانی وضع بھی بہت اہم ہے۔

مشق

1۔ پریکٹیکل کے بعد اطہر کمپیوٹر لیبارٹری سے باہر نکل آیا لیکن اپنا ای میل اکاؤنٹ سائن آف کرنا بھول گیا۔ بعد میں اس کے ہم جماعت ریوان نے اسی کمپیوٹر کو استعمال کرنا شروع کر دیا۔اب وہ اطہر کے طور پر لاگ ان ہے۔ وہ اطہر کے ای میل اکاؤنٹ کا استعمال کر کے اپنے کچھ ہم جماعتوں کو اشتعال انگیز ای میل پیغامات بھیج دیتا ہے۔ ریوان کا یہ عمل مندرجہ ذیل میں سے کون سے سائبر جرم کی مثال ہے؟ اپنے جواب کو مدلل بیان کیجیے۔

a) ہیکنگ
b) شناختی چوری
c) سائبر ہراسانی
d) ادبی سرقہ

2۔ ریشیکا کو اپنی ڈیسک کے نیچے ایک شکن دار اور مڑی ہوئی شکل میں کاغذ کا ایک ٹکڑا ملا۔اس نے اسے اٹھا کر کھولا۔اس میں کچھ متن لکھا ہوا تھا جسے تین مرتبہ کاٹا گیا تھا۔لیکن اسے یہ متن اب بھی آسانی سے سمجھ میں آرہا تھا اور یہ اس کی ہم جماعت گرویت کا ای میل آئی ڈی اور پاس ورڈ تھا۔ ریشیکا کا مندرجہ ذیل میں سے کون سا عمل اخلاقی طور پر صحیح ہے؟

a) گرویت کو اس بارے میں مطلع کرنا تاکہ وہ اپنا پاس ورڈ تبدیل کر سکے
b) گرویت کی ای میل آئی ڈی کا پاس ورڈ اپنے باقی سبھی ہم جماعتوں کو بتانا
c) گرویت کے پاس ورڈ کی مدد سے اس کے اکاؤنٹ کو کھولنا

3۔ سہانا کو بخار ہے لہٰذا اس نے کل اسکول نہ جانے کا فیصلہ کیا ہے۔ اگلے دن شام کو اس نے اپنے ہم جماعت شوریہ کو فون کیا اور کمپیوٹر کلاس کے بارے میں پوچھا۔اس نے اس سے تصور کی وضاحت کرنے کی بھی درخواست کی۔شوریہ نے کہا کہ ''میڈم نے ہمیں یہ پڑھایا کہ پائتھن میں ٹپل کا استعمال کس طرح کرتے ہیں''۔علاوہ ازیں اس نے فیاضی کا مظاہرہ کرتے ہوئے کہا کہ ''آپ مجھے تھوڑا وقت

نوٹ

دیں، میں آپ کو وہ مواد ای میل کروں گا جو پائتھن میں ٹپل کو سمجھنے میں آپ کی مدد کرے گا۔'' شوریہ نے فوراً ہی انٹرنیٹ سے پائتھن میں ٹپل کے تصور کی وضاحت کرنے والا 2 منٹ کا ویڈیو کلپ ڈاؤن لوڈ کرلیا۔ ایک ویڈیو ایڈیٹر کا استعمال کرکے اس نے اس کلپ میں ایک متن ''شوریہ کے ذریعے تیار کردہ'' جوڑ دیا۔ اس کے بعد اس نے یہ ترمیم شدہ کلپ سہانا کو ای میل کردی۔ شوریہ کا یہ عمل مندرجہ ذیل میں سے کس کی مثال ہے؟

a) ایماندارانہ استعمال

b) ہیکنگ

c) کاپی رائٹ کی خلاف ورزی

d) سائبر جرم

4۔ اپنے دوست سے لڑائی کے بعد آپ نے مندرجہ ذیل کام کیے۔ ان میں سے کون سا کام سائبر ہراسانی کی مثال نہیں ہے؟

a) آپ نے اپنے دوست کو ایک ای میل ارسال کیا جس میں لکھا تھا ''میں معذرت چاہتا ہوں''

b) آپ نے اپنے دوست کو یہ کہتے ہوئے ایک دھمکی آمیز پیغام بھیجا کہ ''مجھے کال کرنے یا مجھ سے بات کرنے کی کوشش نہ کریں''

c) آپ نے اپنے دوست کی ایک پریشان کردینے والی تصویر بنائی اور سوشل نیٹ ورکنگ سائٹ پر اپنے اکاؤنٹ میں اپ لوڈ کردی

5۔ سوربھ کو ''ڈیجیٹل انڈیا پہل'' عنوان پر ایک پروجیکٹ تیار کرنا ہے۔ وہ انٹرنیٹ سے معلومات حاصل کرنے کا فیصلہ کرتا ہے۔ وہ ڈیجیٹل انڈیا پہل سے متعلق معلومات پر مشتمل تین ویب صفحات (ویب صفحہ 1، ویب صفحہ 2، ویب صفحہ 3) ڈاؤن لوڈ کرتا ہے۔ سوربھ کے ذریعے اٹھایا گیا مندرجہ ذیل میں سے کون سا قدم ادبی سرقہ یا کاپی رائٹ کی خلاف ورزی کی مثال ہے۔ اپنے جواب کو مدلل بیان کیجیے۔

a) اس نے ویب صفحہ 1 سے ڈیجیٹل انڈیا پہل سے متعلق ایک پیراگراف پڑھا اور اس کے اپنے الفاظ میں دوبارہ فقرے بنائے۔ آخر میں اس نے اس پیراگراف کو اپنے پروجیکٹ میں چسپاں کردیا۔

b) اس نے ویب صفحہ 2 سے ڈیجیٹل انڈیا پہل سے متعلق تین تصاویر ڈاؤن لوڈ کیں اور ان تصاویر کا استعمال کرکے اپنے پروجیکٹ کے لیے ایک کولاج بنایا۔

c) اس نے ویب صفحہ 3 سے ''ڈیجیٹل انڈیا پہل'' آئکن ڈاؤن لوڈ کیا اور اسے اپنی پروجیکٹ رپورٹ کے سرورق پر چسپاں کیا۔

6۔ مندرجہ ذیل کا ملان کیجیے۔

کالم A	کالم B
ادبی سرقہ (Plagiarism)	جعل ساز، نجی معلومات مثلاً بینک اکاؤنٹ وغیرہ سے متعلق معلومات کو حاصل کرنے کے لیے خصوصی انعامات یا رقم کی پیش کش کرتے ہیں
ہیکنگ (Hacking)	انٹرنیٹ سے معلومات واطلاعات کی نقل کرکے اسے اپنی رپورٹ میں شامل کرکے اسے دوبارہ سے ترتیب دینا
کریڈٹ کارڈ سے متعلق دھوکہ دہی	ایسے نشانات جن کی تشکیل اس وقت ہوتی ہے جب کوئی شخص انٹرنیٹ کا استعمال کرتا ہے
ڈیجیٹل فوٹ پرنٹ	نجی ای میل اور دیگر فائلوں کو پڑھنے کے لیے کمپیوٹروں میں نقب زنی

7۔ آپ کو حال ہی میں ہوئے لین دین کے بارے میں آپ کے بینک سے ایک SMS موصول ہوا ہے جیسا کہ شکل میں دکھایا گیا ہے۔ مندرجہ ذیل سوالوں کے جواب دیجیے:

a) کیا آپ دیے ہوئے رابطہ نمبر پر اپنا پن نمبر SMS کریں گے؟

b) کیا آپ موصول ہونے والے SMS کی تصدیق کرنے کے لیے بینک ہیلپ لائن نمبر پر کال کریں گے؟

8۔ پریتی نے اپنے اہل خانہ کے ساتھ اپنا جنم دن منایا۔ وہ خوشی کے ان لمحات کو اپنے دوست ہمانشو کے ساتھ شیئر کرنے کے لیے بے تاب تھی۔ چنانچہ اس نے اپنے جنم دن کی تقریبات سے متعلق چند تصاویر سوشل نیٹ ورکنگ سائٹ پر اپ لوڈ کر دیں تاکہ ہمانشو انھیں دیکھ سکے۔ کچھ دنوں کے بعد پریتی اور ہمانشوں کے درمیان جھگڑا ہو گیا۔ اگلی صبح اس نے سوشل نیٹ ورکنگ سائٹ سے اپنے جنم دن کی ان تصاویر کو ہٹا دیا تاکہ ہمانشو کو ان تصاویر تک رسائی حاصل نہ ہو سکے۔ بعد ازاں شام کے وقت وہ اس وقت حیرت میں پڑ گئی جب اس نے یہ دیکھا کہ جن تصاویر کو اس نے سوشل نیٹ ورکنگ سائٹ سے ہٹا دیا تھا۔ ان میں سے ایک تصویر گایتری کے پاس موجود تھی جو ہمانشو اور پریتی دونوں کی دوست ہے۔ اس نے فوراً ہی گایتری سے دریافت کیا ''یہ تصویر آپ کو کہاں سے ملی؟'' گایتری نے جواب دیا ''ہمانشو نے کچھ دیر پہلے ہی اس تصویر کو فارورڈ کیا تھا۔''

مندرجہ ذیل سوالوں کے جواب تلاش کرنے میں پریتی کی مدد کیجیے۔ اپنے جوابات کو مدلل بیان کیجیے تاکہ پریتی اسے واضح طور پر سمجھ سکے۔

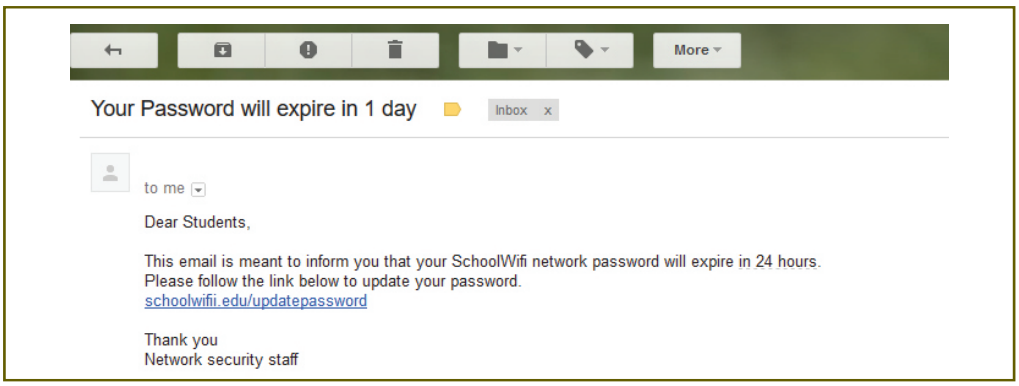
a) ہمانشو نے اس تصویر تک کس طرح رسائی حاصل کی جسے میں نے پہلے ہی حذف کر دیا تھا؟

b) کیا کوئی اور فرد بھی ان حذف شدہ تصاویر تک رسائی حاصل کر سکتا ہے؟

c) کیا ان تصاویر کو میرے ڈیجیٹل فوٹ پرنٹ سے نہیں ہٹا گیا تھا؟

9۔ ایک اسکول میں گیارھویں جماعت کے کمپیوٹر سائنس کے طلبا کو وائرلیس (wifi) سہولت فراہم کی جاتی ہے۔ ترسیل کے لیے اسکول کے نیٹ ورک سکیوریٹی اسٹاف کے پاس ایک رجسٹرڈ یو آر ایل schoolwifi.edu ہے۔ 17 ستمبر 2017 کو ایک ای میل گیارھویں جماعت کے سبھی کمپیوٹر

سائنس کے طلبا کو تقسیم کیا گیا۔ جس میں یہ کہا گیا تھا کہ طلبا کے پاس ورڈ کی معیاد ختم ہونے والی ہے۔ 24 گھنٹے کے اندر اپنے پاس ورڈ کی تجدید کرنے کے لیے URL پر جانے کی ہدایات دی گئی تھیں۔



(a) کیا آپ کو اس ای میل میں کوئی تضاد یا بے قاعدگی نظر آتی ہے؟

(b) اگر طالب علم دیے گئے URL پر کلک کرے گا تو کیا ہوگا؟

(c) کیا یہ ای میل سائبر جرم کی مثال ہے؟ اگر ہاں تو اس بات کی وضاحت کیجیے کہ یہ کس قسم کا سائبر جرم ہے؟ اپنے جواب کو مدلل بیان کیجیے۔

10۔ آپ چھٹیاں منانے کی غرض سے کہیں باہر جانے کا منصوبہ بنانے جا رہے ہیں۔ آپ نے مندرجہ ذیل معلومات حاصل کرنے کے لیے انٹرنیٹ سرفنگ کی ہے۔

(a) موسمی حالات

(b) ایئر ٹکٹ کی دست یابی اور کرایہ

(c) تفریحی مقامات

(d) ہوٹل ڈیل

آپ کے مذکورہ بالا کون سے عمل کی وجہ سے ڈیجیٹل فوٹ پرنٹ کی تشکیل ہوئی ہوگی؟

11۔ آپ اس بات کی شناخت کس طرح کریں گے کہ آپ کے کسی دوست کو سائبر ہراسانی کا نشانہ بنایا جا رہا ہے؟

(a) ایسی آن لائن سرگرمیوں کا ذکر کیجیے جن سے آپ کو یہ معلوم کرنے میں مدد ملے گی کہ آپ کے کسی دوست کو سائبر ہراسانی کا نشانہ بنایا جا رہا ہے۔

(b) اس قسم کی صورت حال سے نمٹنے کے لیے آئی ٹی ایکٹ 2000 (2008 میں ترمیم شدہ) میں کیا بندوبست کیے گئے ہیں؟

12۔ مندرجہ ذیل کے درمیان فرق واضح کیجیے۔

(a) حق اشاعت (کاپی رائٹ) اور پیٹنٹ

(b) ادبی سرقہ اور کاپی رائٹ کی خلاف ورزی

نوٹ

c) غیر اخلاقی ہیکنگ اور اخلاقی ہیکنگ

d) فعال اور غیر فعال فوٹ پرنٹ

e) فری سافٹ ویئر اور فری اور اوپن سورس سافٹ ویئر (FOSS)

13۔ اگر آپ ویب پر کسی مضمون کے مختصر متن کو استعمال کرنے کا منصوبہ بنا رہے ہیں تو استعمال کیے جانے والے ماخذ کو کریڈٹ دینے کے لیے آپ کو کیا اقدامات کرنے چاہئیں؟

14۔ جب آپ آن لائن تصاویر تلاش کرتے ہیں تو آپ ان تصاویر کو کس طرح حاصل کریں گے جو فری پبلک ڈومین میں دست یاب ہیں؟ کاپی رائٹ کی خلاف ورزی کے بغیر ان تصاویر کو آپ اپنے پروجیکٹ میں کس طرح استعمال کریں گے؟

15۔ گھر پر اپنے وائرلیس راؤٹر کو محفوظ کرنا کیوں اہم ہے؟ انٹرنیٹ کی مدد سے معقول حد تک محفوظ پاس ورڈ کی تشکیل کے ضابطے تلاش کیجیے۔ اپنے گھر کے راؤٹر کے لیے ایک خیالی پاس ورڈ بنائیے۔ کیا آپ اپنے ہوم راؤٹر کے پاس ورڈ کو مندرجہ ذیل لوگوں کے ساتھ شیئر کریں گے؟ اپنے جواب کو مدلل بیان کیجیے۔

a) والدین

b) دوست

c) پڑوسی

d) ہوم ٹیوٹر

16۔ مندرجہ ذیل کو یقینی بنانے کے لیے آپ جو اقدامات کریں گے ان کی فہرست بنائیے۔

a) آپ کا کمپیوٹر لمبے عرصے تک صحیح حالت میں کام کرتا رہے۔

b) اسمارٹ اور محفوظ انٹرنیٹ سرفنگ

17۔ ڈیٹا کی خلوت (اخفائے راز) سے کیا مراد ہے؟ آپ جن ویب سائٹس پر جاتے ہیں وہ آپ کے بارے میں کس قسم کی معلومات جمع کرتی ہیں؟

18۔ ایک کمپیوٹر سائنس کی کلاس میں سنیل اور جگدیش کو ان کے استاد نے مندرجہ ذیل کام تفویض کیے۔

a) سنیل سے کہا گیا کہ وہ ''ہندوستان، ایک نیوکلیائی طاقت'' کے موضوع سے متعلق معلومات تلاش کرے۔ اس سے گوگل کروم (Google Chrome) براؤزر استعمال کرنے اور گوگل ڈاکس (Google Docs) کی مدد سے اپنی رپورٹ تیار کرنے کے لیے کہا گیا۔

b) جگدیش سے ''ڈیجیٹل انڈیا'' کے موضوع سے متعلق معلومات تلاش کرنے کے لیے کہا گیا۔ اسے موزیلا فائر فاکس (Mozilla Firefox) کا استعمال کرنے اور لبرے آفس رائٹر (Libre Office Writer) کی مدد سے اپنی رپورٹ تیار کرنے کی ہدایت دی گئی ہے۔

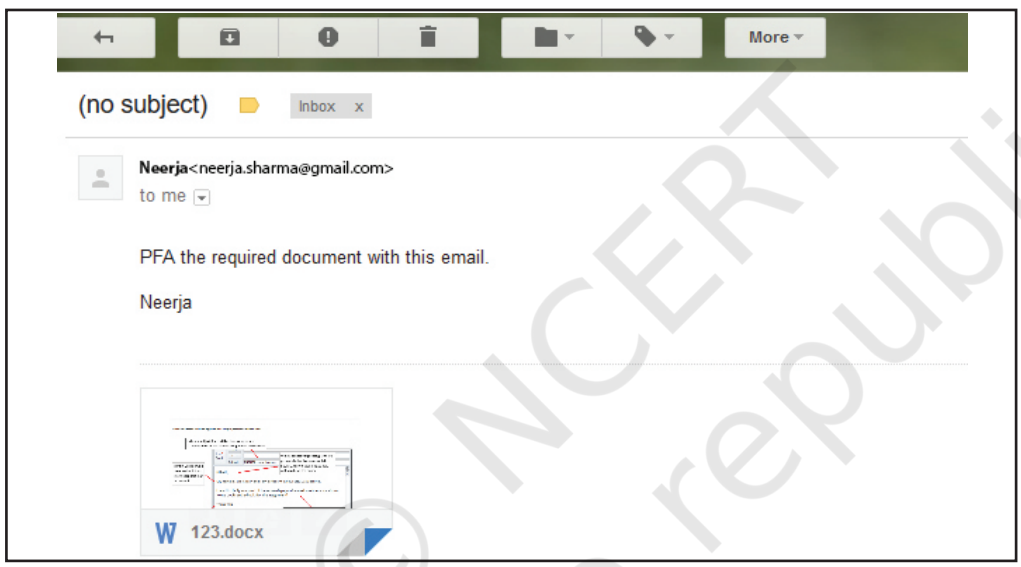
سنیل اور جگدیش کے ذریعے استعمال کی جانے والی ٹیکنالوجی میں کیا فرق ہے؟

19۔ مثالیں دے کر یہ بتائیے کہ آپ مندرجہ ذیل سائبر جرائم کا شکار تھے؟ علاوہ ازیں اس قسم کے سائبر جرائم سے نبرد آزما ہونے کے لیے آئی ٹی ایکٹ میں کیا بندوبست کیے گئے ہیں؟

(a) شناخت کی چوری

(b) کریڈٹ کارڈ اکاؤنٹ کی چوری

20۔ نیرجا گیارھویں جماعت کی طالبہ ہے۔ اس نے کمپیوٹر سائنس کا انتخاب کیا ہے۔ نیرجا نے ایک پروجیکٹ تیار کیا ہے جو اسے تفویض کیا گیا تھا۔ اس نے یہ پروجیکٹ اپنے ٹیچر کو ای میل کے ذریعے ارسال کیا ہے۔ اس ای میل کا اسنیپ شاٹ ذیل میں دیا گیا ہے۔



بتائیے کہ ای میل سے متعلق مندرجہ ذیل میں سے کون سے آداب اس میں موجود نہیں ہیں؟

(a) ای میل کا مضمون

(b) رسمی تسلیمات

(c) خود وضاحتی اصطلاحات

(d) مرسل کی شناخت

(e) آداب

21۔ سمیت نے سبھی مضامین میں اچھے نمبر حاصل کیے ہیں۔ اس کے والد نے اسے تحفے میں ایک عمدہ قسم کا لیپ ٹاپ دیا۔ وہ سمیت کو لیپ ٹاپ کے غیر مناسب اور بہت زیادہ استعمال کی وجہ سے صحت پر پڑنے والے مضر اثرات سے آگاہ کرنا چاہتے ہیں۔ ان نکات کی فہرست تیار کیجیے جن پر اس کے والد کو سمیت سے گفتگو کرنی چاہیے۔

نوٹ

نوٹ