کمپیوټر سیکورټي ۽ اخلاقيات

يونٽ پنجون

شاگردن جي سکيا جي حاصلات

- معمول جي زندگيءَ ۾ ڪمپيوٽر جي سيڪيورٽي جي اهميت وغيره بيان ڪرڻ.
- ڪمپيوٽر تحفظ سان منسلڪ مختلف اصطلاحن جي وصف بيان ڪرڻ.
- حقيقي زندگيءَ جي مثالن سان ڪمپيوٽر سان لاڳاپيل جرمن جي وضاحت ڪرڻ.
- سائيبر اٽيڪس ۽ ان کان بچاءُ جي طريقن جي وصف بيان ڪرڻ.
- سائيبر هراسمينٽ ۽ ان جو شڪار ٿيڻ جي صورت ۾ عملي قدمن کڻڻ تي بحث ڪرڻ.
- ان ڳالهه جي وضاحت ڪرڻ ته سائبر ڪرائم جي خلاف مدد ڪيئن ڪرڻ گهرجي.

5.1 ڪمپيوٽر تحفظ Computer Security

ڪمپيوٽر اسانجي زندگيءَ جو اهم حصو ٿي ويو آهي. اسان ڊاڪيومينٽس، تصويرون، پروگرامز وغيره جي شڪل ۾ ڪمپيوٽر تي ڊيٽا رکون ٿا تنهن ڪري اسان اها اميد رکندا آهيون ته اسانجي معلومات محفوظ هجي ۽ اسانجو ڪمپيوٽر بنا ڪنهن مسئلي جي هلندو رهي. ڪجهه حملا اسان جي ڪمپيوٽرن لاءِ نقصانڪار هوندا آهن. اهي حملا مختلف وائرسز جي شڪل ۾ يا ڪمپيوٽر جي بي ضبط استعمال جي صورت ۾ ظاهر ٿين ٿا. پنهنجي ڪمپيوٽر کي اهڙن حملن کان بچائڻ لاءِ اسان کي ڪمپيوٽر سيڪيورٽيءَ تي عمل ڪرڻو پوندو. ڪمپيوٽر سيڪيورٽي اسانجي ڪمپيوٽر هارڊويئر، سافٽ ويئر ان ۾ موجود انفارميشن جي چوري يا امڪاني نقصان کان تحفظ هوندو آهي.

5.1.1 ڪمپيوٽر سيڪيورٽي جي اهميت Importance of Computer Security

ڪمپيوٽر سيڪيورٽي، اسانجي ڪمپيوٽر جي مجموعي صحت لاءِ بيحد اهم آهي. اها اسانجي معلومات کي محفوظ رکي ٿي ۽ وائرسز ۽ مالويئر (Viruses and Malware) کان بچائي ٿي. ان عمل سان پروگرام تيز ۽ رواني سان هلن ٿا. اها حساس ۽ رازداري واري معلومات کي به بچائي ٿي.

سائنس ۽ ٽيڪنالوجي ۾ اڳيرائيءَ اسان جي روزمره جي زندگيءَ ۾ ڪم ڪار جي طريقن کي بدلائي ڇڏيو آهي. اسان پنهنجا ڪم ڪار ڪرڻ لاءِ موبائل فون ۽ ڪمپيوٽر تي پاڙيون ٿا. ڪمپيوٽر ۽ موبائل فون استعمال ڪندي اسان کيتري ئي اهڙي معلومات به حاصل ڪندا آهيون. جيڪا ٻين سان وندٻڌاهڙ چاهيندا آهيون. ان معلومات ۾ پاسورڊ، بينڪنگ جو تفصيلات، ڪانٽيڪٽس ۽ تصويرون وغيره هوندا آهن. ان معلومات کي محفوظ رکڻ لاءِ، اسان کي پنهنجون ڊوائسز محفوظ (Secure) ڪرٽيون پوندیون آهن ته جيئن کو به ماڻهو اسانجي اجازت کان سواءِ معلومات تائين پهچي نه سگهي ۽ نقصان نه پهچائي سگهجي. ڪمپيوٽر سيڪيورٽي ان ڪري اهم آهي ته ماڻهن کي محفوظ ماحول ۾ ڪم ڪرڻ جو اختيار ڏئي ٿي. اها اهم ترين ڪاروباري عملن ۾ پڻ ڪم ڏئي ٿي. هي ڪجهه سبب آهن جن جي ڪري ڪمپيوٽر سيڪيورٽيءَ کي سنجيدگيءَ سان ڏسڻ گهرجي.

5.1.2 سائبر ڪرائم Cyber Crime

جيئن جيئن مواصلات، واپار ۽ خدمتون ڪمپيوٽر نيٽورڪس تي منتقل ٿيڻ لڳيون آهن، تيئن تيئن سائبر ڪرائم پڻ وڌي رهيا آهن. سائبر ڪرائم اهي جرم آهن جيڪي ڪمپيوٽر نيٽورڪ جي ذريعي ڪيا ويندا آهن. سائبر ڪرمينل ڊوائيسز جو استعمال ڪندي ناجائز طور تي اهم معلومات تائين رسائي حاصل ڪندا آهن. پاسورڊ جي اهم معلومات چورائڻ، سوشل ميڊيا اڪائونٽ هيڪ ڪرڻ، ڪنهن ٻئي جي اڪائونٽ ۾ داخل ٿي وڃڻ ۽ ان مان پئسا ڪڍرائڻ ۽ آنلائن فراڊ ڪرڻ سائبر ڪرائم جا ڪجهه مثال آهن. سائبر ڪرائم غير قانوني ۽ قابل سزا جرم آهي. پاڪستان جي سائبر ڪرائم قانون تحت جيڪو ماڻهو ڪنهن ماڻهوءَ يا اداري جي رازداريءَ سان هٿ چراند ڪندو يا انهن جي وقار کي ڇيهو رسائڻ جي ڪوشش ڪندو ان کي وڏي ڏنڊ سميت ٽن کان پنجن سال تائين قيد جي سزا ملندي.

(i) هيڪرز Hackers

هيڪر اهي ماڻهو هوندا آهن جن کي ڪمپيوٽر، سسٽم، نيٽورڪ ۽ پروگرامن جي گهري ڄاڻ هوندو آهي. هيڪنگ اهو ماڻهو ئي ڪري سگهي ٿو جيڪو پنهنجي واڌارو صلاحيتن سان نيٽورڪ جي ڪمزورين کي ڳولي لهي ۽ انهن تي قابو پائي. هيڪرز مسلسل نئين معلومات حاصل ڪندا رهندا آهن ۽ کين جيڪو به ڪجهه حاصل ٿيندو آهي اهو آساني سان بين سان وندبيندا آهن. هيڪرز کي هروبرو خراب ماڻهو سمجهيو ويندو آهي. جڏهن ته هيڪرز اسان جي نيٽورڪ جي ڪمزورين ۽ تحفظ جي حوالي سان مددگار ثابت ٿي سگهن ٿا. سرڪاري ۽ ڪاروباري ادارا هاڻي ايٿيڪل هيڪرز (Ethical Hackers) کي مقرر ڪري رهيا آهن. انهن جو ڪم ڏيتا جي چوريءَ کي روڪڻ هوندو آهي ۽ کين "وائٽ هيٽ هيڪرز" (White Hat Hackers) يا اڇي ٽوپيءَ وارا هيڪرز چئبو آهي.

(ii) ڪريڪرز Crackers

ڪريڪرز اهي ماڻهو هوندا آهن جيڪي سيني سسٽمز تائين غير قانوني رسائي حاصل ڪري سگهندا آهن. اهي پاسورڊ، ڪمپيوٽر پروگرام جا لائسنس، سورسڪوڊ جهڙن لوازمات کي اورانگهيندي، ڪمپيوٽر سيڪيورٽيءَ کي ٽوڙي سگهندا آهن. هو اهو سڀ منفي نيت سان ڪندا آهن. ڪريڪرز، ڪنهن به مخصوص نيٽورڪ کي غير دستياب يا ناڪاره بنائي سگهن ٿا. هر عام طور تي اهڙا ڪمپيوٽر سسٽم ڪمائڻ لاءِ ڪندا آهن، پر اهي، شهرت لاءِ، مذاق خاطر يا ائين ئي ڪنهن کي ستائڻ لاءِ پڻ ڪندا آهن.

5.1.3 حقيقي زندگيءَ ۾ ڪمپيوٽر ڪرائم Computer Crimes in Real Life

جيئن جيئن ٽيڪنالوجيءَ جو واهپو وڌندو پيو وڃي تيئن تيئن ڏيتا سيڪيورٽي پڻ اهم ٿيندي پئي وڃي. ڪمپيوٽر ڪرائم بين الاقوامي ڏيتا سيڪيورٽي ترسٽ کان ويندي هڪ فرد جي ذاتي نقصان جي انديشي تائين ٿي

سگھي ٿو. 2013ع ۾ هيڪرز هڪ بلين ماڻهن جي ايميل اڪائونٽن کي هيڪ ڪري چڏيو هيو. بالڪل ائين 2017ع ۾ وناڪرائي (Wannacry) وائرس UK جي نيشنل هيلٿ سروس تي حملو ڪيو جنهن جي نتيجي ۾ ڪيترن ئي ڏينهن تائين سسٽم ناڪاره بڻيو رهيو. جيستائين شخصي نوعيت جي جرمن جو تعلق آهي. سوشل ميڊيا ۽ ميل اڪائونٽس کي هيڪ ڪرڻ عام آهي. ڪمپيوٽر ڪرائم جا هاڻي ڪيترائي قسم آهن. جن کي هاڻي سائبر ڪرائم چيو ويندو آهي. انهن مان ڪجهه جرمن جو احوال هيٺ پيش ڪجي ٿو.

(i) هيڪنگ Hacking

ڪمپيوٽر جي دنيا ۾ هيڪنگ سڀ کان وڌيڪ ٿيندڙ جرم آهن. هيڪرز، اسان جي واڌاڻ ايميل ۽ سوشل ميڊيا اڪائونٽ جا پاسورڊ چوراڻي سگھن ٿا. هيڪرز ڪنهن ويب سائٽ تي حملو ڪري ان کي بند ڪرائي سگھن ٿا. جڏهن ته هيڪنگ جو اسڪوپ ان کان گھڻو وسيع آهي. هيڪرز سرڪاري، ڪاروباري ادارن جي حساس معلومات چوراڻي سگھن ٿا. ٽڪي ٿ واريون ٽرانسيڪشن ڪري سگھن ٿا ۽ ڪلائوڊ يا نيٽورڪ ڪمپيوٽرز تان ڊيٽا اڏائي سگھن ٿا.

(ii) ڊيبٽ ۽ ڪريڊٽ ڪارڊ واريون ٽڪيون Credit & Debit Card Scams

ڊيبٽ ڪريڊٽ ڪارڊز جو استعمال اڄڪلهه عام جام آهي پر انهن ڪارڊن جو غير محفوظ استعمال تمام خطرناڪ ٿي سگھي ٿو. جي ڪنهن ماڻهوءَ وٽ اسانجي ڊيبٽ يا ڪريڊٽ جي معلومات آهي ته هو ٽڪي ٿ واري ٽرانسيڪشن ڪري سگھي ٿو، ان معلومات کي حاصل ڪرڻ جا ڪيترائي طريقا ٿي سگھن ٿا. هڪڙو طريقو فراڊ يا اسڪيمرنگ وارو آهي. اسڪيمر مختلف اي ٽي ايم يا ڊيبٽ ڪارڊ مشين ۾ چور مشينون لڳائڻ چڏيندا آهن. اهي مشينون ڊيٽا ڪاپي ڪري ونڊيون آهن، جيڪا اسڪيمرز بعد ۾ غلط استعمال ۾ آڻيندا آهن. ڊيبٽ ۽ ڪريڊٽ ڪارڊ بہ پن (PIN) ڪوڊ ذريعي استعمال ٿيندي آهي. صارفين کي اهو ڪوڊ رازداريءَ ۾ رکڻو هوندو آهي. جي نہ ته ڪوبہ ماڻهو اهي ڪارڊ آنلائن خريداريءَ يا ٻين مقصدن لاءِ استعمال ڪري سگھي ٿو. هن کي فقط توهان جي ڪريڊٽ ڪارڊ جو نمبر PIN ۽ ڪارڊن جي پويان پرنٽ ٿيل سيڪيورٽي ڪارڊ نمبر گھربل هوندو آهي.

(iii) فشنگ Phishing

ڪوڙين ويبسائٽن ۽ غلط ايميل ذريعي ذاتي معلومات حاصل ڪرڻ جي طريقي کي فشنگ چيو ويندو آهي. فشنگ ۾ چور مطلوبہ ماڻهوءَ سان ايميل، ٽيليفون يا ٽيڪسٽ ميسيج جي ذريعي رابطو ڪندا آهن ۽ هن کي يقين ڏيارينداآهن ته هو قانوني ۽ پروسيي لائق آهن. هو ڪيس ان ڳالهه تي قائل ڪندا آهن ته ذاتي سڃاڻپ واري معلومات ڪريڊٽ ۽ ڊيبٽ ڪارڊ جا پاسورڊ ۽ ٻي معلومات کين ڏين. اها معلومات مختلف اڪائونٽس تائين رسائي ڏيندي آهي ۽ ماڻهن جي سڃاڻ کي خطري سان گڏو گڏ مالي نقصان پڻ ٿيندو آهي.

(iv) ڪلڪ جيڪنگ Click jacking

توهان کڏهن اهڙو وڊيو ڏٺو آهي جنهن تي لکيل هجي "او خدايا! توهان کي يقين نه ايندو ته هِن چوڪري جا ڪيو آهي." يا کڏهن کا اهڙي ويبسائيٽ جيڪا توهان کي چوندي هجي ته ڪِلڪ ڪري وڏو انعام حاصل ڪيو جيڪو توهان کي گهربل به هوندو. اهو هڪ قسم جو فراڊ آهي، جنهن کي ڪِلڪ جيڪنگ چئبو آهي. خاص طور تي ان ۾ فرادي هارن يا سيڪرٽ انٽرنيٽ صارفين کي نشانو بنائي کين مالوئير جي لنڪ موڪليندا آهن يا ڦِڪي ۽ سان سندن ذاتي معلومات ۽ سوشل ميڊيا سائيٽس ذريعي حاصل ڪندا آهن.

(v) سائبر بليئنگ يا هراسمينٽ Cyber Bullying or Harassment

ڪمپيوٽر، موبائل فون يا انٽرنيٽ جهڙا اليڪٽرانڪ ذرائع آنلائن بليئنگ يا هراسمنٽ جي لاءِ استعمال ٿيندا آهن. ڏمڪي آميز روين (Bullying Behavior) ۾ افواهه پکيڙڻ، ڏمڪائڻ، غير موزون رايا ڏيڻ، ذاتي معلومات ليڪ ڪرڻ، بليڪ ميل ڪرڻ، نفرت آميز گفتگو وغيره اچي وڃن ٿا. ان ۾ مرڪزي مطلوبه ماڻهوءَ کي نقصان پهچائڻ جي نيت هوندي آهي. نتيجي طور، متاثر ماڻهو، ذاتي نقصان، خودڪشيءَ جي ارادي ۽ ۾ ٻين کيترين ئي مسئلن ۽ جذباتي روين جو شڪار ٿيندو آهي. جن ۾ دٻجي وڃڻ، ذهني الجهاءَ جو شڪار ٿيڻ، چڙ ڏيکارڻ، ڊپريشن جو شڪار ٿيڻ غيره اچن ٿا.

5.1.4 سائبرائٽيڪ Cyber Attack

جڏهن ڪو سائبر ڏوهاري ڪمپيوٽر يا ڪنهن ٻئي ذريعي سان ڪنهن اڪيلي يا گهڻن نيٽورڪس تي حملو آور ٿئي ته اهڙي قدم کي سائبر اٽيڪ چئبو آهي. ڏوهاري ڪريڪنگ، اسڪيم لنڪس، فشينگ يا ڪنهن ٻئن ذريعن سان ڪمپيوٽر نيٽورڪ ۾ داخل ٿيندو آهي. عام طور تي سائبر حملي کو مفاد حاصل ڪرڻ لاءِ يا متاثر ڪمپيوٽر، نيٽورڪ يا ويبسائيٽ کي نقصان پهچائڻ لاءِ ڪيا ويندا آهن. سائبر اٽيڪ يا تهنشانو بنيل ڪمپيوٽر کي ناڪاره بنائي ڇڏيندو آهي يا معلومات اڏاري ڇڏيندو آهي، يا وري ان کي آنلائن ڪري ڇڏيندو آهي. اهو ڪمپيوٽر يا نيٽورڪ تان معلومات چورائي به سگهي ٿو.

5.1.4 متاثر ٿيڻ جي صورت ۾ ڇا ڪرڻ گهرجي؟

سائبر ڪرائم ڪرڻوارو مجرم مهميشي لکي رابطو ڪرڻ لاءِ چوندو آهي جي نه ته سنگين نتيجا پوڻ پوندا. سائبر ڪرائم بليئنگ يا هراسمينٽ جي شڪار ماڻهوءَ جو جواب تمام اهم هوندو آهي. اهڙن مسئلن مان جان ڇڏائڻ جا طريقا آهن. پهريون ڪم ته اهو ڪرڻو هوندو آهي ته پروسي لائق ماڻهوءَ کي ٻُڌائجي جيڪي گهڻو ڪري استاد يا والدين تي سگهن ٿا.

سائبر بلينئگ ۾ هراسمينٽ جهڙن سائبر ڪرائيمز کي منهن ڏيڻ سرڪار پڻ اقدام ڪنيا آهن. پاڪستان ۾ سائبر ڪرائيم جي شڪار ماڻهن جي مدد لاءِ نيشنل ريسپانس سينٽر فار سائبر ڪرائمز (National Response Center for Cyber Crimes) قائم ڪيو ويو آهي. ويبسائيٽ تي موجود فارم جي مدد سان آنلائن ڪمپلين ڪري سگهجي ٿي يا وري هفتي جا ست ڏينهن چوبيه ئي ڪلاڪ ڪليل هيلپ لائن نمبر 9911 تي رابطو ڪري مدد ونڊي سگهي ٿي.

شڪل 5.1
سائبر ريسڪيو هيلپ لائن

شاگردن جي سکيا جي حاصلات

- ڪمپيوٽر وائرس جي وصف ۽ ان کان بچاءَ جا طريقا بيان ڪرڻ.
- وائرس جي مختلف قسمن جي وصف ۽ منجهن تفريق ڪرڻ، جهڙوڪ، مالوئير، وورم، وائرس، ايڊوئير، اسپائي ويئر.
- وائرس وورم، اسپائي ويئر ۽ ايڊويئر جي مختلف پکڙجڻ جي طريقن کي سڃاڻڻ
- اهو سڃاڻڻ ته اسين وائرس سافٽويئر جهڙوڪ، Avast ، Norton, Moafeee ۽ ٻيا وائرس کان بچاءَ ۾ مددگار ثابت ٿي سگهن ٿا.

5.2 مالويئر Malware

مالويئر لفظ (Malicious Software) جو اختيار آهي. مالوئير هڪ وسيع ترم آهي، جنهن ۾ ڪمپيوٽر جا وائرس، ورمز، اسپائي ويئر، ايڈويئر ۽ ٻيا اچن ٿا. مالويئر بنيادي طور تي هڪ پروگرام هوندو آهي. جيڪو مسئلا پيدا ڪرڻ لاءِ ناهيو ويندو آهي. اهي ايترا خطرناڪ ٿي سگهن ٿا ته ڊوائس هارڊويئر کي به نقصان پهچائي سگهن ٿا. پر ڏهن پر عام طور تي مالويئر ڊيٽا کي خراب يا ختم ڪندا آهن، ڪمپيوٽنگ، مرڪزي عمل کي متاثر ڪندا آهن يا مختلف سرگرمين کي ڊسٽرب ڪندا آهن.

5.2.1 مختلف مالوئير

مالوئير جي قسمن ۾ وائرسز، وورمز، ايڈو ۽ اسپائي ويئر اچن ٿا.

(i) ڪمپيوٽر وائرس Computer Virus

ڪمپيوٽر وائرس هڪ ڪمپيوٽر وائرس آهي، جيڪو پنهنجون ڪاپيز ناهيندو ڪمپيوٽرز نيٽورڪز ۾ داخل ٿي پکڙجندو آهي. جنهن جي عام طور تي صارف کي خبر ناهي پوندي. هي بين ڪمپيوٽر پروگرامز ۾ ردوبدل ڪندو آهي. انهن ۾ پنهنجا ڪوڊ داخل ڪري ڪمپيوٽر جي سيٽنگز کي بدلائي ڇڏيندو آهي. وائرس نقصانڪار هوندا

آهن. اهي اسڪرين تي تنگ ڪندڙ پيغام وري وري ڊيڪارڻ کان وٽي سپ ڊاڪيومينٽس يا تہ گم ڪري ڇڏيندا آهن يا اڏائي ڇڏيندا آهن. وائرس عام طور تي هوسٽ فائل ۾ هوندا آهن. جيئن متحرڪ ٿيندا آهن تہ بين فائلز ۽ پروگرامز ۽ ڊاڪيومينٽس ۾ داخلا ٿيندا ويندا آهن. وائرس جا قسم هي آهن. بوٽ سيڪٽر (Boot Sector)، ريزيڊنٽ (Resident)، ميڪرو وائرسز (Macro Virus) ۽ فائلر انفيڪٽر (File Infector).

(ii) ورم Worm

هي هڪ وائرس جو قسم آهي جيڪو هڪ ٻئي ڪمپيوٽر کان ٻئي ڪمپيوٽر تائين پنهنجون ڪاپيز ٺاهي پکڙبو آهي. ورم، ڪنهن ماٺهوءَ جي سست اندازيءَ، کان سواءِ پاڻ ئي پنهنجون ڪاپيز ٺاهيندو آهي. ان کي ڪنهن پروگرام يا فائل کي نقصان پهچائڻ لاءِ ڪنهن فائل سان داخل ٿيڻ جي ضرورت ئي ڪونہ پوندي آهي. اهو ڪيترائي نقصان ڏيڻ وارا ڪم ڪري سگهي ٿو، جيئن اضافي بالوئير کي ڪمپيوٽر ۾ داخل ڪرڻ، ڊوائيسز مٽان پاڻ کي ڪاپي ڪري رکڻ، متاثر سسٽم سان طبعي ڳانڍاپو قائم ڪرڻ، فائل آنلائن، ۽ انٽريل استوريج، ميموري ذريعن کي استعمال ڪرڻ وغيره.

(iii) ايڊويئر Adware

ايڊويئر هڪ ايڊورٽائيزنگ سپورٽ ڪرڻ وارو سافٽويئر آهي. اهي بيشمار ايڊز ۽ پاپ اپ ونڊوز پيدا ڪندا آهن. جنهن سان ميموري ۽ پروسيسنگ ذريعي متاثر ٿيندا آهن. ايڊويئر، انٽرنيٽ برائوزر جون سيٽنگز پاڻ تبديل ڪندو آهي جهڙوڪ هوم پيج ۽ سرچ انجن متائي ڇڏڻ وغيره.

عام طور تي هي ايترا خطرناڪ ناهن هوندا جيترا ٻيا مالويئر هوندا آهن. پر تنهن جي باجود بہ هي صارف کي تنگ ڪندا آهن ۽ پروسيسنگ جي رفتار کي سُست ڪري ڇڏيندا آهن. اها ايڊورٽائزمينٽ ڪنهن وقت پاپ اپ جي صورت ۾ ظاهر ٿيندي آهي. ڪڏهن وري نندڙيون ونڊوز ٺهنديون آهن. جن کي بند ڪرڻ ممڪن ناهي هوندو. ايڊويئر پروگرامز ۾ گيمز، ڊيسڪٽاپ ٽول بار ۽ يوٽيليٽز هوندا آهن. عام طور تي ايڊويئر ويب تي مبني هوندو آهي. ۽ ويب برائوزر تان، خاص طور تي پاپ ايس ۾ ايڊورٽائز ڈيٽا لاءِ ڊيٽا ڪٽندو آهي.

(iv) اسپائيوئر Spyware

اسپائيويئر اهو مالوئير آهي جيڪو ڊوائس کي مانيٽر ڪندي، ماٺهوءَ جي ذاتي معلومات، سندس مرضيءَ کان سواءِ چورائي، ٻئي ماٺهوءَ يا اداري کي موڪليندو آهي. اسپائي ويئر موبائل فون يا ڪمپيوٽر تي، ائين ڪنٽرول ڪندو آهي، جو صارف کي ان جي خبر بہ ناهي هوندي. اهو ويب برائوزنگ هسٽري، ايميل ميسيج، يوزرنيم، پاسورڊ

۾ آنلائن پيمينٽ جي معلومات چوري ڪندو آهي. اسپائي ويئر ڪوڪيز جي ذريعي يا وري ان وقت ڪمپيوٽر ۾ داخل ٿيندا آهن جڏهن ڪو پروگرام انسٽال ڪندي، ان جي ٽرمس ۾ ڪنڊيشنز کي پڙهڻ کان سواءِ راضپو ڏيکاريندا آهيون. اسپائي ويئر جا ڪجهه مثال هي آهن، سسٽم مانيٽرز (System Monitors)، ڪوڪيز ٽريڪرز (Cookies Trackers)، روٽڪٽس (Rootkits)، ڪي لاگرز (Key Loggers) وغيره.

5.2.2 وائرس جي ڦهلاءَ جا ذريعا

ڪمپيوٽر وائرس بہ فلو وائرس وانگر آهي. ان کي ائين ٿاهيو ويندو آهي ته هڪ ڪمپيوٽر کان ٻئي تائين پهچي ۾ پاڻ کي منتقل ڪندو رهي. جيڪا بہ ڊوائس وائرس متاثر هوندي اها ٻين ڊوائسز کي متاثر ڪندي. ان جو مطلب ته وائرس ٻاهران ايندا آهن. ڪيئن ايندا آهن؟ ان جا ڪجهه طريقا هيٺ ڏجن ٿا.

(i) يو ايس بي فليش ڊسڪ ۽ سي ڊيز USB Flash Disk & CD's

يو ايس بي فليش ڊوائسز، فائلن کي ٽرانسفر ڪرڻ جو سڀ کان عام ذريعو آهي. هڪ وائرس متاثر سسٽم هڪ صاف شفاف يو ايس بي ۾ وائرس منتقل ڪندو آهي ۽ بلڪل ائين هڪ متاثر يو ايس بي هڪ صاف شفاف ڪمپيوٽر ۾ وائرس منتقل ڪندو آهي. ونڊوز ۾ موجود آٽورن (Auto-Run) پروگرام، سي ڊي يا فليش ڊسڪ لڳائڻ شرط ڪم ڪرڻ شروع ڪندو آهي. اهو عمل وائرس کي ڪمپيوٽر ۾ پکيڙڻ جو سبب بڻبو آهي. اهو متاثر ڪنڊ فائل ڪاپي ڪندو ڪمپيوٽر ۾ منتقل ڪندو آهي.

(ii) انٽرنيٽ ڊائونلوڊ مينيجر Internet Download Manager

ڪمپيوٽر وائرس انٽرنيٽ تان ڊائونلوڊ ٿيندڙ فائلز يا سافٽويئرز جي ذريعي بہ پکڙجي سگهن ٿا. انٽرنيٽ منجهان داخل ٿيندڙ وائرس بہ اسانجي ڪمپيوٽر کي هيڪرز جي هٿن ۾ ڏئي سگهن ٿا. جيتوڻيڪ هر اينٽي وائرس سافٽويئر، وائرس جو شڪار ڊائونلوڊ ڪان بچاءَ جي ڊال ڏيندا آهن. ان جي باوجود بہ اهو ضروري آهي ته فائل ۽ ڊائونلوڈ ڪنهن پروسي لائق ذريعن تان ڪئي وڃي.

استادن لاءِ هدايت

استاد کي ٽراجن هارس، روٽ ڪيٽ، بيڪڊور اس ۽ بوٽس وغيره ۾ اهڙن وائرسن جي ڄاڻ ڏيڻ گهرجي. انهن کي اسائنمينٽ طور ڏئي سگهجي ٿو.

(iii) کمپيوٽر نيٽورڪ Computer Network

صارفين کي محتاط رهڻ گهرجي ته لوڪل ايريا نيٽورڪس (LAN) مان ڪنهن فائل پڙهڻ يا ڪمپيوٽرن کي نقصان ڏيڻ سگهن ٿا. ساڳيوئي مسئلو بلوٽوٿ ذريعي هڪ موبائل کان ٻئي موبائل ۾ ڏيڻ يا موڪلڻ دوران ٿي سگهي ٿو.

(iv) ايميل اٽيچمينٽ Email Attachment

شڪل 5.2 وائرس ايميل اٽيچمينٽس ذريعي پکڙجي سگهي ٿو

وائرسز پکيڙڻ جي اهم ذريعي ۾ ايميل اٽيچمينٽ پڻ مشهور آهي. ايميل اٽيچمينٽس ذريعي هڪ ڪمپيوٽر کان ٻئي ڪمپيوٽر تائين وائرس آساني سان پکڙجي سگهي ٿو. متاثر ڪندڙ مواد ڪنهن ڪوڙيءَ يا اڻڄاتل ايميل ذريعي اچي سگهي ٿو. مجرم چاڪندا آهن جو يا ته ڪوڙي آءِ ڊي ذريعي يا سچي آءِ ڊيءَ مان هڪ ٻاڪر متائي، ان ذريعي وائرس موڪليندا آهن. اسانجي رابطن ۾ موجود ماڻهو به اسان کي اهڙو متاثر ڪندڙ مواد موڪلي ٿا سگهن جنهن جي کين به مواد جي خبر ناهي هوندي. صارفين کي گهرجي هر ايميل ۾ ايندڙ مواد يا لنڪ کي ڪِلڪ ڪرڻ کان پهرين ايميل جي اصليت ضرور چيڪ ڪن. خاص طور تي اسپيس ميل ۾ آيل اٽيچمنٽس کي وڏي ڏيان سان کولڻ گهرجي.

5.2.3 اينٽي وائرس Anti-Virus

اينٽي وائرس، ڏيٽا يا هارڊ ويئر کي درپيش ممڪن نقصان کان بچائڻ لاءِ خاص طور تي ڊزائن ٿيل يوٽلٽي پروگرام آهن. صارفين کي اهو پرزور مشورو ڏجي ٿو ته ونڈوز جهڙي آپريٽنگ سسٽم تي اينٽي وائرس پروگرام ضرور انسٽال ڪجي. اينٽي وائرس پروگرام پسمنظر ۾ هلندو آهي. هر هڪ هلندڙ سافٽويئر ۽ انٽرنيٽ تان ايندڙ ڏيٽا ايپل جو جائزو وٺندو آهي. ڪنهن به مشڪوڪ سرگرمي جي صورت ۾ اينٽي وائرس صارف کي ايڪشن ڪٽڻ لاءِ آگاهه ڪندو آهي. عام طور تي اينٽي وائرس فائلن کي وائرس سان پاڪ ڪندو آهي ۽ جي صاف نه ٿي سگهيو ته متاثر فائلن کي الڳ ڪري رکي ڇڏيندو آهي. اهو به مشورو ڏجي ٿو ته صارف پنهنجي اينٽي وائرس کي معمول مطابق اپڊيٽ ڪندو رهي. ڪيترائي اينٽي وائرس انٽرنيٽ تي موجود آهن جن مان گهٽا ته بلڪل مفت ۾ ملندا آهن. تڏهن به مفت وارن اينٽي وائرس پروگرام ۾ تازا فيچرز ناهن هوندا. پيسا پريندڙ صارفين کي پريميئر صارف چيو ويندو آهي. انهن کي سيڪيورٽي جا تازا فيچرز ڏنا ويندا آهن.

عام ترين اينٽي وائرس هي آهن.

(i) Avast

Avast دنيا جي وڏين سيڪيورٽي ڪمپنين مان هڪ آهي. اواست جي انتظاميہ جي اها دعوي آهي تہ هو وقت کان اڳ پري ٽيڪنالاجي ذريعي حقيقي وقت ۾ سائبر حملن کان بچڻ جي تحفظ ڏين ٿا. هنن جي اها دعوي پڻ آهي تہ هن وٽ ڪلائوڊ تي مبني هڪ مشين لرننگ انجن آهي جيڪا ڪروڙين صارفين جي ڊيٽا کي مسلسل حاصل ڪندي رهي ٿي اها وائرسز جي تيز ترين سڃاڻ کي ممڪن بنائي ٿي ۽ هٿرادو ذهانت (Artificial Intelligence) کي بهتر ۽ وائرس جي خلاف مؤثر بنائي ٿي.

شڪل 5.3 اينٽي وائرس Avast

(ii) Norton

نارٽن اينٽي وائرس 1991ع کان مشهور آهي. هي سيڪيورٽي، يوٽيلٽي سافٽويئرز جي هڪ وڏي خاندان سمنٽيڪ ڪارپوريشن جو حصو آهي. نارٽن اينٽي وائرس استعمال ۾ بالڪل آسان آهي ۽ منجهس اهڙيون ڪانفيگيوريشن آهن، جيڪي ماهرن کي گهربل هوندیون آهن. هن کي ٽيسٽنگ ليبس پاران ڪيل چڪاس ۾ سڀ کان متاهين ريٽنگ وارو سافٽويئر ڄاڻايو ويو آهي ۽ ان کي اهڙيءَ طرح ڊزائن ڪيو ويندو آهي جو توهان جي سسٽم جي ڪارڪردگيءَ تي گهٽ کان گهٽ اثر وجهي.

شڪل 5.4 اينٽي وائرس Norton

(iii) McAfee

McAfee جي دعوي آهي تہ هو اينٽي وائرسس، برائوسس ۽ سڃاڻ جي تواز ۽ فيچرز جو مجموعو آڇيندا آهن. هن صارفين کي جديد وائرسز، مالويئر، رينسمويئر ۽ اسپائي ويئر حملن کان بچائيندو آهي. ۽ انهن جي سڃاڻپ جي رازداري پڻ بچائيندو آهي.

شڪل 5.5 اينٽي وائرس McAfee

5.2.4 مالوئير کان بچاءُ

مالويئر ۽ وائرس کان بچڻ اسانجي پنهنجي هٿ ۾ هوندو آهي. 90% کان وڌيڪ ڪمپيوٽر صارفين جي غلطين جي سبب متاثر ٿيندا آهن. اسان جو ڪمپيوٽر سست ٿي ويو آهي. يا ان جي ڪارڪردگيءَ تي اثر ٿي رهيو آهي؛ پراسيسز جي دوران بيهي رهي ٿو يا گهٽا پيراري اسٽارٽ ٿئي ٿو. غير ضروري پيغام اچڻ شروع ٿين ٿا ڊاڪيومينٽ ۽ فائل غائب ڪري ڇڏي ٿو ته مطلب ان کي وائرس لڳي ويو آهي. اسان کي اهڙي صورتحال پيدا ٿيڻ کان بچڻ گهرجي. هي ڪجهه عام اقدام آهن. جن سان اسان پنهنجي سسٽم کي وائرس ۽ مالويئر کان بچائي سگهون ٿا.

شڪل 5.6 شيبول اسڪين
نقصان کان محفوظ رکي سگهي ٿو

- اينٽي وائرس سافٽويئر انسٽال ڪري ان کي اپڊيٽ ڪندا رهو.
- اينٽي وائرس سافٽويئر جي مدد سان روزانو سسٽم اسڪين ڪندا رهو.
- پنهنجي OS کي اپڊيٽ رکو.
- اهي انٽرنيٽ لنڪس جنتي غير معمولي قسم جا ليبل، فوٽو يا ڪيپشن هجن، انهن تي ڪلڪ ڪرڻ کان پرهيز ڪيو.
- اڻڄاڻ ماڻهن پاران موڪليل ايميل اٽيچمينٽس ۽ هائپر لنڪس تي ڪلڪ نه ڪيو.
- يو ايس بي فليش ڊسڪ، SD ڪارڊ ۽ موبائل فون کي استعمال ڪرڻ کان پهرين اسڪين ڪيو.
- غير ضروري پاپ اپس ۽ انسٽنٽ ميسيجز کان بچاءَ جي لاءِ اسپيم بلاڪ ۽ فلٽرنگ ٽولز استعمال ڪيو.
- انٽرنيٽ تان فقط پروسي جي لائق ذريعن تان مواد ڊائون لوڊ ڪيو.
- ڪوبه اوپن وائي فائي ڪڏهن به استعمال نه ڪيو.

5.2.5 بيڪ اپ ڊيٽا رکڻ

اسان کي پنهنجي ڊيٽا جي امڪاني ڏيان کان بچڻ لاءِ پڻ ڪجهه اقدامات ڪرڻ گهرجن ان جا ڪجهه طريقا هيٺ ڏجن ٿا.

- سسٽم ريسٽور پوائنٽ هر روز ڏسندا رهو ۽ ان کي ناڪاره نه ٿيڻ ڏيو.

- اهم ڊيٽا کي سي ڊي يا ڊي وي ڊي تي ڪاپي ڪري رکو. جيئن تہ اهي محفوظ هوندیون آهن. ان ڪري انهن ۾ وائرس ناهي وجي سگهندو.
- اهم فائلن جو بيڪ اپ، هڪ کان وڌيڪ جاين تي رکو.
- توهان پنهنجي ڊيٽا کي گوگل ڊرائيو ۽ مائڪروسافٽ ڊرائيو جهڙن ڪلائوڊ اسٽوريج تي پڻ بيڪ اپ ڪيو.

شاگردن جي سکيا جي حاصلات

- آٿينٽيڪشن مڪينزم جي وضاحت ڪرڻ.
- آٿينٽيڪشن مڪينزم جي مختلف طريقن جي لسٽ ترتيب ڏيڻ.
- يوزر سيس پاسورڊ، پرسنل آئڊنٽيفيڪيشن نمبر ۽ بائيوميٽرڪ آٿينٽيڪيشن مڪسزم ۾ فرق بيان ڪرڻ.

5.3 آٿينٽيڪيشن مڪينزم Authentication Mechanism

هي ۽ هارڊويئر ۽ سافٽويئر تي مبني هڪ سيڪاٽپ جو مڪينزم آهي، جيڪو ڊوائس ۾ اندر ڊيٽا تائين رسائي ۽ کان پهرين اسان جي سڃاڻ جي پڪ ڪندو آهي.

5.3.1 سيڪيورٽي مڪينزم جا قسم

صارف جي سڃاڻ کي ممڪن بنائڻ لاءِ ڪيترائي ڪمپيوٽر سيڪيورٽي سسٽم آهن انهن مان ڪجهه هيٺ ڏجن ٿا.

(i) يوزرنيم ۽ پاسورڊ Username and Password

يوزرنيم ۽ پاسورڊ ، ڪوڈز جو جوڙو هوندا آهن. جن جي صارف کي خبر هوندي آهي اهي صارف جي سڃاڻ ڪرڻ جو ڪم ڪندا آهن. اڄ جي دور ۾ ويب تي، صارف جي سڃاڻ لاءِ يوزرنيم پاسورڊ تي ڊفالٽ طريقيڪار آهن. تڏهن بہ ڪجهه جديد وڌن ڪمپيوٽر حملن، يوزرنيم ۽ پاسورڊ وارن سڃاڻ جي طريقي کي ناقابل قبول بنائي ڇڏيو آهي. ان سان گڏ مڪمل سڃاڻ جي لاءِ اضافي سڃاڻ جا طريقا پڻ لاڳو ڪيا ويا آهن.

(ii) پرسنل آئڊنٽيفيڪيشن نمبر Personal Identification Number (PIN)

شڪل 5.7 پرسنل آئڊنٽيفيڪيشن نمبر

PIN جو مطلب آهي ذاتي سڃاڻ جو انگ يا Personal Identification Number هي توهان جي سڃاڻ جي پڪ ڪرڻ جو هڪ

سيڪيورٽي ڪوڊ آهي. هي پاسورڊ وانگر هوندو آهي، جنهن کي پڙ رازداريءَ ۾ رکڻ گهرجي. جو ته هي توهان جي رازداراڻي ايميل ۽ مالي ٽرانسيڪشن جهڙن اهم معاملن ۾ استعمال ٿيندا آهن. ڊيبٽ يا ڪريڊٽ ڪارڊ جي چوريءَ يا گم ٿيڻ جي صورت ۾ PIN تحفظ ڏيندا آهن، جو ته PIN کان سواءِ ڪابه ٽرانسيڪشن نه ٿي ڪري سگهجي.

(iii) بائيوميٽرڪ تصديق Biometric Verification

شڪل 5.8 آڱرين جي نشانين ۽ اک جي پتلي جي سڃاڻ

بائيوميٽرڪ تصديق، Authentication طريقي ڪار کان مختلف آهي. هي پهرين تصديق ڪندي آهي ته اصلي صارفئي ڏيڻا يا ڊوائيس تائين رسائي حاصل ڪري سگهي. بائيوميٽرڪ تصديق ماڻهوءَ جي منفرد بائيوميٽرڪ نشانين تي انحصار ڪندو آهي. بائيوميٽرڪ تصديق حقيقي وقت ۾ ڏيڻا حاصل ڪري ان کي جديد سسٽم تي موجود ڏيڻا سان پيٽائي ڏسندو آهي. جڏهن بائيوميٽرڪ جي ڏيڻا ٻئيميس جڙيندو آهي ته پوءِ تصديق مڪمل ٿيندي آهي. بائيوميٽرڪ جو عام ترين استعمال آڱرين جي نشانين (Finger Print) جي اسڪينگ وارو آهي. جڏهن ته ڪجهه جديد سسٽم ۾ اکين، اک جي پتلين، منهن ۽ آواز جي سڃاڻ جا طريقا پڻ موجود آهن.

شاگردن جي سکيا جي حاصلات

- ڪمپيوٽر جي ميدان جي پيشاوراڻي اخلاقيات جي اهميت بيان ڪرڻ
- مصدقہ معلومات جي وضاحت ڪرڻ
- انٽيليڪچوئيل پراپرٽي حقن جي مختلف قسمن Patents، Copyrights ۽ Trademarks جي وضاحت بيان ڪرڻ
- سافٽويئر پائريسي (Software Piracy) ۽ ان جي اثرات جي وضاحت ڪرڻ.
- معلومات جي رازداريءَ جي وضاحت ڪرڻ.
- پليجيئرزم (Plagiarism) تي بحث ڪرڻ

5.4 ڪمپيوٽر جي ميدان ۾ پيشاورانه اخلاقيات

Professional Ethics in the Field of Computer

ڪنهن پيشي جي حوالي سان شخصي شاندارائي قانون جيڪي رويي جي رهنمائي ڪنائهن کي پيشآور اخلاقيات يا Professional Ethics چئبو آهي. ڪنهن پيشي متعلق ٽائيم ٽيبل پيشاوراڻي ضابطي جو فريم ورڪ جيڪو قدر ۽ قانون پڻ جوڙيندو آهي. ڪمپيوٽنگ پروفيشنلز جا عمل دنيا کي تبديل ڪندا آهن. ڪين پنهنجي ڪم

جي وسيع ڪارج تي غور فڪر ڪرڻ گھرجي تہ جيئن سندن ڪم لڳاتار عوامي پلائي لاءِ استعمال ٿئي. ان لاءِ ڪجھ رهنما اصول هيٺ ڏجن ٿا.

- انساني ۽ سماجي پلائيءَ ۾ ڪردار ادا ڪرڻ ۽ اهو پڻ تسليم ڪرڻ تہ ڪمپيوٽنگ ۾ سيئي ماڻهو پائيوار آهن.
- ايمانداريءَ سچائيءَ سان ڪم ڪرڻ
- ساز و سامان جي عزت ڪرڻ
- نقصان پهچائن کان پرهيز ڪرڻ
- ڪنهن بہ قسم جي تفريق، نڪي يا هراسمينٽ ڪرڻ کان پرهيز ڪرڻ
- نون، خيالن، ايجادن تخليقي ڪم ۽ اخلاقي عمل لاءِ گھربل ڪم جي عزت ڪرڻ
- رازداري برقرار رکڻ ۽ رازداري جو احترام ڪرڻ.
- پيشاوارائٽ روين، مهارتن ۽ اخلاقي عملن جي عمده معيارن تي عمل ڪرڻ
- بين فردن ۽ گروهن جي واڌاري ۽ ترقيءَ لاءِ موقعا فراهم ڪرڻ
- شخصي ۽ بين ذريعن کي ورڪ لائف کي بهتر ڪرڻ لاءِ استعمال ڪرڻ.
- ان جي پڪ ڪرڻ تہ مجموعي طور ڪمپيوٽنگ جي ڪم جو مقصد مفاد عام آهي
- ڪمپيوٽنگ ۾ مواصلاتي ذريعن تائين اجازت سان رسائي حاصل ڪرڻ
- ماڻهن ۾ ڪمپيوٽنگ ۽ ان سان لاڳاپيل ٽيڪنالوجيز جي واهپي ان جي نتيجن جي آگاهي کي وڌائڻ.

5.4.1 معلومات جي تصحيح جي وصف ڪرڻ
Define Information Accuracy

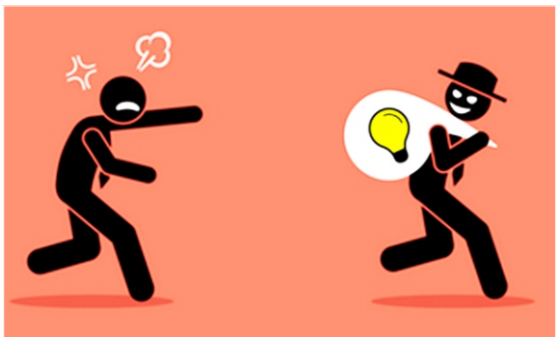
معلومات جي تصحيح اهو قدم آهي جنهن سان معلومات جي سچي ۽ صحيح هجڻ جي تصديق ڪري سگھجي. اهو بہ ضروري آهي تہ بي اعتمادي واري ڊيٽا منجهان معلومات اخذ نہ ڪجي. معلومات جي تصحيح لاءِ ضروري آهي تہ معلومات کي پروسيس لائق ذريعن سان پيٽائجي.

معلومات جي دؤر ۾ اسان کي معلومات حاصل ڪرڻ لاءِ اڳتي وڌائڻ ۾ بي حد احتياط کان ڪم وٺڻ گھرجي. خاص طور تي سوشل ميڊيا تي موجود معلومات جو صحيح هجڻ هميشہ سوالیہ هوندو آهي.

شڪل 5.9 معلومات جي تصحيح

5.4.2 انٽيليڪچوئل پراپرٽي جا حق Intellectual Property Rights

جڏهن ڪو ماڻهو ڪو سافٽويئر ٺاهي، ڪتاب لکي، تحقيقي مقالو لکي يا ڪا سيشن يا طريقه ڪار تخليق ڪري، تہ اهو ان شخص جي ڏاهپ ميراث يا انٽليڪچوئل پراپرٽي (Inflated Property) سڏائيندو آهي. ڏاهپ جو ميراث انساني ذهانت جي تجريدي تخليق آهي. ٻين ملڪيتن وانگر ڏاهپ جي ملڪيت ۾ چوري ٿي سگهي ٿي. ڏاهپ جي ملڪيت کي چوريءَ يا غلط استعمال يا ڦهلائڻ کان بچائڻ لاءِ ڏاهپ جي ملڪيت جو حق (Intellectual Property Right) استعمال ٿيندو آهي. انهن حقن جي ذريعي، ڪاپي رائٽس، پيٽنٽس ۽ ٽريڊ مارڪس وسيلي، ڏاهپ جي ملڪيت کي بچائي سگهجي ٿو. اهي پيٽينٽس، ٽريڊمارڪس يا ڪاپي رائيٽ اڳ ۾ ٽيل ڪم جي مالڪن کي پنهنجي ڪم يا لاڳت جي تحفظ جو اختيار ڏيندا آهن. انهن حقن تحت، ڪو به ماڻهو يا ادارو اجازت کان سواءِ ڪنهن جي انٽيلڪچوئل پراپرٽيءَ کي ڪاپي يا استعمال نہ ٿو ڪري سگهي. ڏاهپ جي ملڪيت جا حق سڄي دنيا ۾ استعمال ٿيندا آهن. پاڪستان به International Property Organization ڏاهپ سان لاڳاپيل حقن جي نظرداري ڪندو آهي.



شڪل 5.10 انٽيليڪچوئل پراپرٽي جو خيال رکڻ گهرجي

(i) پيٽنٽ Patent

شڪل 5.11 پيٽنٽ

پيٽنٽ ڪنهن به ايجاد جي ٺاهڻ، استعمال ڪرڻ ۽ وڪڻڻ لاءِ محدود عرصي تائين مليل اختياري حق آهي. پاڪستان ۾ ان جو مدو ويهه سال آهي. پيٽنٽ جو حق رکڻ واري کي اختيار آهي تہ پنهنجي ايجاد (تخليق) کي ٺاهڻ، وڪڻڻ يا استعمال ڪرڻ کان ڪنهن کي به روڪي سگهي. هائير ايجوڪيشن ڪميشن شاگردن ۽ اسڪالرز جي تحفظ لاءِ IPO سان پيٽنٽ رجسٽريشن کي سپورٽ ڪري ٿو. پيٽنٽ جو طريقو نئون آهي، جديد طريقي سان ان کي عمل ڪري ٿو ۽ صنعت ۾ پڻ استعمال ڪري سگهجي ٿو.

(ii) ڪاپي رائيٽ Copy Right

شڪل 5.12 ڪاپي رائيٽ

هي هڪ قانوني حربو آهي جنهن جي مدد سان فن پارو ۽ ادب يا ڪو به معلومات يا خيال وندڻ وارو تخليقڪار پنهنجي تخليق کي محفوظ ڪندو آهي. سادن لفظن ۾ هي ڪاپي

ڪرڻ جو استحقاق آهي. ڪاپي رائيٽ جو مقصد اهو هوندو آهي ته معلومات جي واڌاري جي لاءِ، ڪم جي تخليقڪار کي معاشي فائدو ڏنو ويندو آهي. ©جي نشاني عام طور تي ڪاپي رائيٽ وارين شين کي لڳل هوندي آهي.

(iii) ٽريڊ مارڪ Trademark

ٽريڊ مارڪ ڪنهن شيءِ يا خدمت کي سڃاڻڻ جي باقي شين ۽ خدمتن کان الڳ ڪندو آهي. ٽريڊمارڪس بہ انٽيليڪچوئل پراپرٽي رائٽس تحت محفوظ ٿيندا آهن. جنهن جو مطلب آهي تہ ڪا شيءَ يا خدمت ڪنهن مخصوص ماڻهوءَ يا اداري جي ملڪيت آهي. هي ڪو بہ فهم جو ڳو اصطلاح، لفظ، لوگو يا ڪا نشاني ٿي سگهي ٿي ۽ ان کي TM سان ظاهر ڪيو ويندو آهي. TM ادارن کي سندن شيون جي لوڪل ۽ گلوبل مارڪيٽ تائين رسائيءَ ۾ مدد ڏيندو آهي. ٽريڊ مارڪ ناهڻ بہ هڪ تخليقي ڪم آهي ۽ پيشہ آور طريقي سان ٿيندو آهي. ٽريڊ مارڪ ناهڻ لاءِ ڪيترائي سافٽويئر موجود آهن.

شڪل 5.13 ٽريڊ مارڪ رجسٽري

5.4.3 سافٽويئر جي چوري Software Piracy

سافٽويئر يا پائريسي جي معني آهي ڪنهن ڪاپيرائيٽيڊ سافٽويئر جو غير قانوني استعمال ڪاپي يا وڪرو ڪرڻ. هيءُ عمل سافٽويئر انڊسٽري کي درپيش تمام وڏو خطرو آهي. اهو سافٽويئر ناهيندڙ ۽ وڪرو ڪندڙ لاءِ وڏي پئماني تي نقصان جو سبب بڻجي سگهي ٿو. پائريسي جي ڪري اصلي سافٽويئر وڪرو ڪندڙ وٽ ايترا پئسا ناهن هوندا جو هر ان ميدان ۾ ٽيندڙ نئين تحقيق کي هٿي وٺرائي سگهن. جيئن تہ ڪين تمام گهٽ فائدو ملندو آهي. ان ڪري هو ڳريون قيمتو نصارفين جي مٿان مڙهڻ تي مجبور ٿي پوندا آهن.

سافٽويئر جي ڪمپنين مختلف حربا استعمال ڪري ڏٺا آهن تہ سافٽويئر جي چوري يا ڪاپي کان بچي سگهجي، پر انهن مان اڪثر ناڪام ويا آهن. هنن ڪاپي تحفظ جي لاءِ بہ اڀيرائي ڪئي جنهن ۾ صارف کي پروگرام هلائڻ لاءِ ڪا Key لڳائڻي پوندي آهي. اڄ جي دور ۾ هر ڪو سافٽويئر آنلائن رجسٽر ٿئي ٿو. پر ان جي باوجود بہ سافٽويئر جي ڪاپي رکي ناهي سگهي.

چوري ڪيل سافٽويئر جو استعمال صارفين لاءِ پڻ خطرناڪ آهي. قانوني نتيجن پويان ڳڻ جو خوف پنهنجي جاءِ تي چوريءَ وارو سافٽويئر استعمال ڪندڙ صارف، سافٽويئر جي اهم فيچرز کان پڻ محروم هوندا آهن. چوري يا ڪاپي ٿيل سافٽويئر ڪنهن بہ وقت ڪم ڇڏي سگهي ٿو، يا ڪم کي صحيح انداز سان سرانجام نہ ٿو ڏئي سگهي. ان

کان علاوہ چوري ٹيل سافٹويئر استعمال ڪرڻ وارا صارف، قانوني مدد، اپگريڊ، ٽيڪنيڪل مواد، تربيت ۽ بگ فڪسز کان پڻ محروم رهندا آهن.

5.4.4 پليجريزم Plagiarism

ڪنهن ليکڪ يا تخليقار جا خيال سندس نالو ٻڌائڻ کانسواءِ، پنهنجي نالي سان پيش ڪرڻ کي پليجرزم چئبو آهي. اڪيڊمڪ ايمانداريءَ جي اها گُهر آهي ته ڪنهن جو به خيال، لفظ يا ڊيٽا کي استعمال ڪرڻ وقت انهن اصلوڪن مالڪن جو نالو ضرور ٻڌائجي پليجرزم هڪ بداخلاقي آهي ۽ ان جا اگرا نتيجا نڪري سگهن ٿا. ڪالیجون ۽ يونيورسٽيون شاگردن کي پابند ڪنديون آهن ته هو پنهنجو ذاتي ڪم پيش ڪن ۽ جيڪڏهن ڪنهن ٻئي جا خيال، لفظ ۽ ڪم ٻڌائن ٿا تہ ان جا مڪمل ضابطي اندر حوالا ضرور قلمبند ڪن. جي هو اهو نہ ڪري سگهيا تہ انهن تي ڏنڊ لڳي سگهي ٿو. پليجرز جي مسئلن کان بچڻ لاءِ آنلائن طريقيڪار به آهي. تعليمي ادارا پليجرزم کي سڃاڻڻ واريون خدمتون خريد ڪندا آهن. انهن مان سڀ کان وڌيڪ استعمال ٿيندڙ خدمت ترنيٽن (Turnitin) آهي.

خلاصو

- ڪمپيوٽر جو تحفظ مطلب، ڪمپيوٽر هارڊويئر، سافٽويئر ۽ ان ۾ موجود معلومات کي چوري ٿيڻ يا امڪاني طور نقصان يا وائرس جي حملي کان بچائڻ.
- سائبر ڪرائم اهو جرم آهي جيڪو ڪمپيوٽر ۽ نيٽورڪ جي ذريعي ڪيو وڃي.
- هيڪرز پنهنجي صلاحيتن کي استعمال ڪندي ڪنهن به نيٽورڪ جي ڪمزورين کي ڳولينداآهن.
- ڪريڪرز اهي ماڻهو آهن جيڪي ڪنهن به ٻئي سسٽم تائين غير مصدقہ رسائي حاصل ڪندا آهن.
- Phishing جو مطلب آهي ته ڪوڙين ايميلز ۽ ويبسائيٽس ذريعي ڪنهن جي ذاتي ڄاڻ تائين رسائي حاصل ڪرڻ.
- ڪنهن کي ڊيڄارڻ، ڌمڪائڻ ۽ هراس ڪرڻ لاءِ ڪمپيوٽر ۽ موبائل فون جهڙا الیڪٽرانڪ ذريعا پڻ استعمال ٿيندا آهن.
- جڏهن سائبر مجرم ڪمپيوٽر يا پي ڪا ڊوائس جا استعمال ڪندي ڪنهن ٻئي ڪمپيوٽر يا نيٽورڪ ۾ داخل ٿي وڃي ته ان کي سائبر اٽيڪ چئبو آهي.
- سائبر حملي جو شڪار ٿيل ماڻهوءَ کي ڪنهن اعتماد واري ماڻهوءَ يا سرڪاري اداري سان ڳالهه ڪرڻ گهرجي.
- مالويئر يا متاثر سافٽويئر هڪ وسيع اصطلاح آهي، جنهن ۾ ڪمپيوٽر وائرس، Worms، اسپائي ويئر، ايڈويئر ۽ ٻيا مسئلا پيدا ڪندڙ پروگرام اچن ٿا.
- وائرس يا سالويئر يو ايس بي فليش ڊسڪ سي ڊي، انٽرنيٽ ڊائونلوڊنگ، ڪمپيوٽر نيٽورڪ ۽ ايميل اٽيچمينٽس ذريعي پکڙبو آهي.
- اينٽي وائرس يوٽلٽي پروگرام خاص پروگرام آهن جيڪو ڪمپيوٽر ڊيٽا يا هارڊويئر کي وائرس ۽ مالويئر جي خطرن کان بچائيندو آهي.
- ڊيٽا جي تحفظ جي لاءِ ان جو هڪ ڪاپي وڌيڪ جاين تي بيڪ اپ رکي ڇڏبو.
- تصديق وارو طريقيڪار، هارڊ ويئر سافٽويئر سان لاڳاپيل طريقيڪار هوندو آهي جيڪو اها تصديق ڪندو آهي ته فقط اصلي صارف ڊيٽا تائين رسائي ٿي سگهن.
- پيشاورائي اخلاقيات مطلب اهي ذاتي ۽ ڪارپوريٽ اصول ۽ ضابطا جيڪي پيشي کي هڪ مربوط روين کي احاطي ۾ رکڻ لاءِ ٺهن.
- معلومات جي تصحيح اهو حربو آهي جنهن سان درپيش ۽ سچي معلومات جو تعين ڪري سگهجي.

- ڏات جي ميراث يا ملڪيت انساني ذهانت جي تجريدي تخليق آهي. ڏات جي ملڪيت جي چوري، غلط استعمال يا وڪري کان بچڻ لاءِ انٽيلڪچوئل پراپرٽي رائيٽ جو اسـتعمال ٿيندو آهي. انهن حقن ذريعي پيٽنٽس، ڪاپي رائيٽس ۽ ٽريڊ مارڪس کي استعمال ڪندي ڏات جي ملڪيت کي بچائي سگهي ٿو.
- سافٽويئر جي چوري معني، ڪاپي رائٽ ٽيل سافٽويئر جو غير قانوني استعمال، نقل يا وڪرو ڪرڻ.
- پليجرزم مطلب ٻئي ڪنهن جي ڪم يا خيال کي ان جي نالي ڏيڻ بجاءِ، پنهنجي نالي سان پيش ڪرڻ.

مشق

(الف) صحيح جواب چونڊيو

1. اهو وسيع اصطلاح جنهن ۾ مختلف نقصانڪار سافٽويئر هوندا آهن، انهن کي..... چئبو آهي.

(الف) وائرس (ب) اسپائڈيٽر (ج) مالويئر (د) ايڈويئر

2. تصديق جو طريقو ڪار جنهن ۾ فقط اصلي صارف تي ڀيٽا تائينرسائي هوندي آهي، ان کي .....چئبو آهي.

(الف) يوزرنيم پاسورڊ (ب) اسڪين ڪوڊ (ج) بائيوميٽرڪ (د) PIN

3. سافٽويئر گهٽو..... تحت محفوظ ڪيا ويندا آهن.

(الف) Potent (ب) ڪاپي رائٽس (ج) ٽريڊ مارڪ (د) لوگو

4. ڪمپيوٽر ۾ پيشاوراڻي اخلاقيات ان ڪري اهم آهي جو.....

(الف) اها قانون طور ضروري آهي. (ب) ان جي لتاڙ جا سنجيده نتيجا نڪرن ٿا.

(ج) اها مثبت ۽ صحتمند ڪم جو ماحول ٺاهي ٿي. (د) معاشي فائدن لاءِ ضروري آهي..

5. مرفت جو اينٽي وائرس اڪثر.....

(الف) ڪجهه عرصي ڪانپوءِ ناڪاره ٿي ويندو آهي. (ب) صرف محدود خدمت آڇيندو آهي.

(ج) ان کي اپڊيٽ نه ٿو ڪري سگهجي. (د) اهو خريد نه ٿو ڪري سگهجي.

6. ڪنهن مواد کي انٽرنيٽ تان ڪاپي ڪري ان جي اصلي مالڪ جو حوالو نه ڏيڻ ..... جو مثال آهي.

(الف) پليجريزم (ب) پيٽنٽ جو غير قانوني استعمال

(ج) معلومات جي رازداري (د) ڪاپي رائيٽ جي لتاڙ

7. جيئن تہ اهو ڪا ڊيٽا ڪاپي يا چوري ناهي ڪندو ان کي سيني ڪان گهٽ نقصانڪار..... مالويئر آهي.

(الف)وائرس (ب)ايڊويئر (ج)اسپائي ويئر (د)ٽراجن

8. مالويئر جيڪو پنهنجا نقل ڪندو آهي ۽ ٻئي فائل سان ڳنڍيل ناهي هوندو اهو..... آهي.

(الف)وائرس (ب)ايڊويئر (ج)اسپائيويئر (د)ورم

9. وائرس ڇا جي ذريعي پکڙبو آهي؟

(الف)ايميل اٽيچمنٽ (ب)انٽرنيٽ ڊائونلوڊ (ج)فليش ڊسڪ سي ڊي (د)سيني ذريعي

10. "لنڪ تي ڪلڪ ڪيو 5 ڊالر جو ميڪڊونلڊ وائوچر حاصل ڪيو" هي ڇا جو مثال آهي؟

(الف)اسڪيم (ب)فشنگ (ج)ڪلِڪ جيڪنگ (د)هيڪنگ

(ب) هيٺين جا جواب ڏيو

1. ڪمپيوٽر سيڪيورٽي ڇو اهم آهي؟ ٽي سبب لکو.
2. سائبر بليئنگ کي مثال سان سمجهايو.
3. معلومات جي تصحيح ڇو اهم آهي؟
4. ايٿيڪل هيڪنگ ڇا ٿيندي آهي؟
5. توهان جو ڪو دوست سائبر هراسمينٽ جو شڪار ٿيو آهي، توهان هن کي ڪهڙا به مشورا ڏيندا؟
6. ايميل اڪائونٽ هيڪنگ کان بچڻ لاءِ ڪهڙا به قدم کڻجن؟
7. سافٽويئر پائريسي، سافٽويئر ڊولپرز لاءِ ڇو هاڃيڪار آهي؟
8. فشنگ جا به مثال لکو؟
9. ڏاهپ جي ملڪيت جو حق ڇا آهي؟
10. هيٺ ڏنل ڪرائيٽريا تحت هيٺين ۾ فرق بيان ڪيو؟

ڪرائيٽيريا	وائرس	ورم	ايڊويئر	اسپائي ويئر
خطري جي سطح				
ڪيئن شروع ٿيندو آهي				
هارڊويئر سافٽويئر کي نقصان ڏيئي سگهي ٿو				
ڪمپيوٽر رفتار تي اثر				
پکيڙ جو ذريعو				

(ب) ڪالم پيٽيو

نمبر	الف	نمبر	ب	ج
(i)	ڪنهن ٻئي جا خيال پنهنجا ڪري پيش ڪرڻ.	(الف)	ايڈويئر	
(ii)	اهو ايڈورٽائيزنگ سافٽويئر جيڪو پاپ اپ ونڈوز استعمال ڪري وائرس پکيڙيندو آهي.	(ب)	ڪريڪر	
(iii)	ڪمپيوٽر سسٽم ذريعي ٿيندڙ جرم جو نالو آهي	(پ)	PIN	
(iv)	اهو رازدار اڻوڪو ڊ جيڪو صارف جي سڃاڻ ڏيندو آهي.	(پ)	اينٽي وائرس	
(v)	اهو ماڻهو جيڪو پاسورڊ بائي پاس ڪندي ٻين جي ڪمپيوٽر ۾ داخل ٿيڻ.	(پ)	پليجريزم	
(vi)	اهو يوٽلٽي سافٽويئر جيڪو ڊيٽا کي ٻئي نقصان کان بچائي.	(ت)	سائبر ڪرائم	

سرگرميون

سرگرمي 1 :

پوسٽر نمائش جو اهتمام ڪيو جنهن ۾ شاگرد حاضرين کي ڪمپيوٽر ۽ انٽرنيٽ محفوظ طريقي سان استعمال ڪرڻ جو ٻڌائين ڪجهه تاپڪ هي ٿي سگهن ٿا .

- پنهنجي ڪمپيوٽرن کي وائرس ۽ مالويئر کان بچايو .
- سائبر بليئنگ ۽ هراسمينٽ کان پرهيز ڪيو .
- پائريسي ۽ پليجرم کان پرهيز ڪيو .
- سائبر ڪرائيمز سان ڪيئن نبيرو ڪجي ؟

سرگرمي 2 :

ڪلاس ۾ بحث دوران هي صورتحال شاگردن جي سامهون رکو ڪين ڇئو ته ٻڌائن ته اهڙين حالتن ۾ ڇا ڪرڻ گهرجي؟ ۽ ڇو ڪرڻ گهرجي؟

- توهان کي هڪ فون ڪال اچي ٿي ڪال ڪرڻ وارو توهان کي چوي ٿو ته توهان جو هڪ وڏو انعام نڪتو آهي ۽ توهان تائين انعام پهچائڻ لاءِ ايڊوانس رقم گهربل آهي.
- توهان کي هڪ اٽڇاڻ ايميل آءِ ڊي تائين ايميل اچي ٿي، جيڪا توهان کان بينڪ اڪائونٽ، ايميل ۽ پاسورڊ گهري ٿي.
- ڪا اٽڇاڻ ويبسائيٽ وزٽ ڪندي، ويبسائيٽ توهان کان فيسبڪ گوگل اڪائونٽ جا تفصيل گهري ٿي.

سرگرمي 3 :

انهن خدمتن جي لسٽ ٺاهيو جيڪي مفت جي اينٽي وائرس ۾ ناهن ملنديون.

سرگرمي 4 :

اخبارون انٽرنيٽ ذريعي ڪا سائبر ڪرائم جي ڪا شئي ڳولي لهو. خاص طور تي اها جنهن ۾ ملزم پڪڑيو ويو هجي ۽ ڪيس سزا ملي هجي.

سرگرمي 5 :

ٽيسز ۽ تحقيقي مقالا Turnitin جي ذريعي چيڪ ٿيندا آهن، جيڪا هڪ ٻئينموني انٽرنيٽ تي ملندڙ سروس آهي، جنهن ذريعي پليجرزم جي سڃاڻ ٿيندي آهي. اهڙيون ٻيون به آنلائن خدمتون آهن جي پنهنجي ڊاڪيومنٽ ۽ پليجرزم چيڪ ڪري سگهن ٿيون.

ڪجهه لنڪس هي آهي.

www.duplichcate.com
www.guetext.com
www.hageen.com

ڪنهن به ٽاپڪ تي مضمون لکو. مواد جو ڪجهه حصو انٽرنيٽ تان ڪاپي ڪري مضمون ۾ لڳايو ۽ پوءِ پنهنجي مضمون جو پليجرزم چيڪ ڪيو.