



کمپیوٹر کی حفاظت اور اخلاقیات



معلومات حاصل ہو جاتی ہیں جنہیں ہم دوسروں کو بتانا نہیں چاہتے۔ ان معلومات میں ہمارا پاس ورڈ (Password)، بینک کی تفصیلات، رابطے، تصاویر وغیرہ شامل ہو سکتی ہیں۔ ان معلومات کی حفاظت کے لیے ہمیں اپنی ڈیوائس کو محفوظ بنانا چاہیے تاکہ کوئی بھی ہماری اجازت کے بغیر معلومات کو تباہ و برباد نہ کرے یا پھر ان معلومات کو ہماری اجازت کے بغیر حاصل کر لے۔

کمپیوٹر کی حفاظت اہم ہے کیونکہ یہ لوگوں کو محفوظ ماحول میں اپنا کام انجام دینے دیتی ہے۔ یہاں وہ چند وجوہات دی جا رہی ہیں جن کی وجہ سے کمپیوٹر کی حفاظت کو سنجیدہ لینا چاہیے۔

5.1.2 سائبر کرائم

جیسا کہ مواصلات، تجارت اور خدمات کمپیوٹرز اور نیٹ ورک پر بہت زیادہ بھروسہ کرنے لگی ہیں اس کے ساتھ ساتھ سائبر کرائم بھی اور زیادہ بڑھ گئے ہیں۔ سائبر کرائم وہ کرائم یا جرم ہے جو کمپیوٹر اور نیٹ ورک کے ذریعے کیا جاتا ہے۔ سائبر کرائم ان اہم معلومات تک رسائی کے لیے ڈیوائس استعمال کرتا ہے جس کا اسے کوئی حق نہیں ہوتا۔ پاس ورڈ اور اہم معلومات کو چرانہ، ہیکنگ، سوشل میڈیا اکاؤنٹ، کسی دوسرے کے اکاؤنٹ تک رسائی حاصل کرتا اور ٹرانسیکشن کرنا، آن لائن فراڈ کرنا، جرائم کی چند مثالیں ہیں۔ سائبر کرائم غیر قانونی ہے اور سزا کے قابل ہے۔ پاکستان کے سائبر کرائم کے قانون کے مطابق کوئی بھی مجرم جو کسی شخص یا آرگنائزیشن کے ذاتی جذبات کو مجروح کرے اور ان کی عزت کو نقصان پہنچائے اس کو تین سے پانچ سال تک کی جیل اور بھاری جرمانہ ادا کرنا ہوگا۔

(i) ہیکرز

ہیکر وہ شخص بھی ہو سکتا ہے جسے کمپیوٹر سسٹم، نیٹ ورکس اور پروگرامز کی بہت زیادہ معلومات ہوں۔ ہیکر وہ مرد یا عورت ہو سکتی ہے۔ جو اپنی بہت زیادہ مہارتوں کو استعمال کر کے نیٹ ورک کے اندر موجود قانون یا ضابطے سے بچنے کی صورت نکالتے ہیں۔ ہیکرز مستقل آگے کی معلومات حاصل کرتے رہتے ہیں۔ اور انہوں نے جو کچھ معلومات حاصل کی ہیں انہیں لوگوں کو بتاتے رہتے ہیں۔ ہیکرز عام طور پر خراب افراد سمجھے جاتے ہیں لیکن ہیکرز ہمیں کوائف کی بہتری اور نیٹ ورک کی حفاظت میں بھی

مقاصد خاص SLO



- روزمرہ زندگی میں کمپیوٹر کی حفاظت کی وضاحت کیجئے۔
- کمپیوٹر کی حفاظت سے متعلق مختلف اصلاحات کی تعریف بیان کیجئے۔
- حقیقی زندگی سے مثالیں دے کر کمپیوٹر کے جرائم کی وضاحت کیجئے۔
- سائبر حملے کی وضاحت کیجئے اور یہ بتائیے کہ ان سے کس طرح بچا جائے۔
- سائبر ہیر سمٹ پر گفتگو کیجئے اور اگر ہم اس کا شکار ہو جائیں تو ہمیں کیا کرنا چاہیئے۔
- وضاحت کیجئے کہ سائبر جرائم کے خلاف کس طرح سے مدد حاصل کی جائے۔

5.1 کمپیوٹر کی حفاظت

کمپیوٹر ہماری زندگی کا اہم حصہ بن گیا ہے۔ ہم اپنے کوائف کمپیوٹر میں دستاویزات، تصاویر اور پروگرام وغیرہ کی شکل میں اپنے کمپیوٹر پر جمع کرتے ہیں۔ اس لیے ہماری خواہش یہ ہوتی ہے کہ ہم اپنے سارے کوائف بہ حفاظت رکھیں اور ہمارا کمپیوٹر کسی مسئلے کے بغیر درست طور پر چلے۔ بعض دھمکیاں ہمارے کمپیوٹروں میں کچھ مسائل پیدا کر سکتی ہیں۔ یہ دھمکیاں مختلف اقسام کے وائرس یا کمپیوٹر کا غیر قانونی استعمال ہیں۔ ہمیں اس لیے بدستور کمپیوٹر کی حفاظت کے قوانین پر عمل کرنا چاہیئے۔ اور چوری یا کمپیوٹر کی ہارڈ ویئر، سوفٹ ویئر اور اس پر موجود معلومات کی چوری یا اس کے ٹوٹ پھوٹ جانے سے بچانا یا حفاظت کرنی چاہیئے۔

5.1.1 کمپیوٹر کی حفاظت کی اہمیت:

کمپیوٹر کی حفاظت ہمارے کمپیوٹر کی مکمل صحت یابی کے لیے ضروری ہے۔ یہ ہماری معلومات کی حفاظت کرتی ہے۔ اور وائرل، سزاور malware پروگرام کو زیادہ تیزی اور ہمواری کے ساتھ چلنے دیتا ہے۔ یہ خفیہ اور حساس معلومات کی حفاظت کرتا ہے۔ سائنس اور ٹیکنالوجی میں ترقی نے ہمارے طرز زندگی کو بدل کر رکھ دیا ہے۔ ہم کمپیوٹرز اور موبائل فونز پر کئی سرگرمیاں کرنے کے لیے بھروسہ کرتے ہیں۔ جب ہم کمپیوٹر ز اور موبائل فونز استعمال کرتے ہیں تو ہمیں ایسی بہت ساری

(ii) کریڈٹ اور ڈیبٹ کارڈ کا چکمہ یاد دھوکے بازی

ڈیبٹ یا کریڈٹ کارڈ کو رکھنا بہت عام ہے لیکن ان کا غیر محفوظ استعمال خطرناک ہو سکتا ہے۔ اگر کسی شخص کے پاس ہمارے کریڈٹ یا ڈیبٹ کارڈ کی معلومات ہیں تو پھر وہ فراڈ کے ذریعے اُن اکاؤنٹ میں سے پیسے نکلا سکتا ہے۔ ان معلومات کو حاصل کرنے کے بہت سے طریقے ہو سکتے ہیں۔ ان میں سے ایک طریقہ Scamming ہے۔ ہیکرز ATM یا کریڈٹ کارڈ مشین کے اندر چھوٹی مشین کو سیٹ کر دیتے ہیں۔ یہ مشین کوائف کی نقل کر دیتے ہیں جسے Scammers بعد میں غلط طور پر استعمال کرتے ہیں۔ ڈیبٹ اور کریڈٹ کارڈ بھی PIN کوڈ کے ذریعے محفوظ ہیں۔ استعمال کرنے والے کو اس کوڈ کو خفیہ رکھنا ہوتا ہے ورنہ کوئی بھی شخص اسے آن لائن شوپنگ یا دوسرے مقاصد کے لیے استعمال کر سکتا ہے۔ اُسے صرف ہمارے کریڈٹ کارڈ نمبر، پن اور سیکیورٹی کوڈ کو جاننے کی ضرورت ہے جو کارڈ کے پیچھے لکھا ہوتا ہے۔

Phishing(iii)

یہ حملے ای میل کے ذریعے اور ویب سائٹس کے ذریعے معلومات حاصل کرنے کا ایک طریقہ ہے Phishing کرنے والے اپنے ٹارگیٹ سے رابطہ قائم کرتے ہیں۔ ایسا وہ ای۔ میل، ٹیلی فون، یا تحریری پیغام کے ذریعے کرتے ہیں اور ایسا بن جاتے ہیں کہ وہ قانونی اور قابل بھروسہ شخص ہیں۔ وہ جسے نشانہ بناتے ہیں اُس سے حساس کوائف جیسا کہ اُن کی شخصیت کی شناخت کی اہم معلومات، بینکنگ اور کریڈٹ کارڈ کی تفصیلات اور مختلف وجوہات کی بناء پر Password مانگتے ہیں۔ اُس کے بعد اس معلومات کو استعمال کر کے مختلف اکاؤنٹس تک رسائی حاصل کر لیتے ہیں اور اسکے نتیجے میں شناختی چوری اور مالی نقصان پہنچاتے ہیں۔

Click Jacking(iv)

کیا آپ نے کبھی ایسی ویڈیو دیکھی ہے جس پر OMG آپ یقین نہیں کر سکتے کہ اس لڑکے نے کیا کیا ہے؟ کانٹیکٹ لگا ہو۔ یا آپ کو ویب سائٹ پر ایسا بن ملے گا جو آپ سے کہے گا کہ آپ یہاں کلک کریں اور ایسے انعام کو لینے کا دعویٰ کریں جس کے لیے آپ نے کبھی بھی درخواست نہیں کی ہوگی۔ یہ ایک قسم کا فراڈ ہے جسے Click Jacking کہتے ہیں۔ عام طور پر مجرم بچوں اور

مدد دے سکتے ہیں۔ گورنمنٹ اور تجارتی ادارے اب اخلاقی ہیکرز کو نوکر رکھ رہے ہیں جنہیں سفید ہیٹ والے ہیکرز کہا جاتا ہے۔ یہ کوائف کے چوری ہونے کو بچاتے ہیں۔

(ii) کرکیز

کرکیز وہ اشخاص ہوتے ہیں جو دوسرے سسٹم تک غیر قانونی طور پر مداخلت کرتے ہیں۔ یہ کمپیوٹر کے پروگرام کا پاس ورڈ (Password) یا لائنس کو نظر انداز کر کے، ذرائع کے کوڈ کو تبدیل کر دیتے ہیں۔ کرکیز جس بھی سسٹم کو نشانہ بنائیں اُسے غیر مہیا کر دیتے ہیں یا کام کرنے کے قابل نہیں چھوڑتے۔ یہ ان سرگرمیوں کو عام طور پر پیسے کمانے کے لیے کرتے ہیں اس طرح بین الاقوامی طور پر کمپیوٹر کی حفاظت کو نقصان پہنچاتے ہیں یا ایک چیلنج سمجھ کر یا محض خوشی کرتے ہیں۔

5.1.3 حقیقی زندگی میں کمپیوٹر کے جرائم

جیسے جیسے ٹیکنالوجی پر وان چڑھ رہی ہے کوائف کی حفاظت بھی نہایت اہم ہو گئی ہے۔ ہم بھی کمپیوٹر کے جرائم کا کسی بھی وقت نشانہ بن سکتے ہیں۔ کمپیوٹر کے جرائم کی حد بین الاقوامی کوائف کی حفاظت کی دھمکیوں سے لیکر ذاتی حملے، جارحانہ اقدام یا دل آزاری تک ہو سکتی ہے۔ 2013ء میں، ہیکرز نے ایک ارب ای میل استعمال کرنے والے اکاؤنٹ کو ہیک کر لیا۔ بالکل اسی طرح سے 2017ء، Wanna Cry وائرس کے لے یونائیڈڈ کنگڈم میں قومی صحت کی خدمات پر حملہ کیا جسکی وجہ سے پورا نظام کئی دن تک کے لیے ناکارہ ہو گیا۔ جہاں تک کہ ذاتی جرائم کا تعلق ہے، سوشل میڈیا اور خط و کتابت کے اکاؤنٹ کی ہیکنگ عام ہے۔ جہاں تک کہ ذاتی جرائم کا تعلق ہے، سوشل میڈیا اور خط و کتابت کے اکاؤنٹ کو ہیک Hack کرنا بہت عام ہے۔ کمپیوٹر کے جرائم کی بہت سی اقسام ہیں جنہیں اب ساہر کرائم کہتے ہیں۔ حقیقی زندگی سے متعلق جرائم پر یہاں بحث کی جا رہی ہے۔

(i) ہیکنگ

ہیکنگ کمپیوٹر کی دنیا میں سب سے زیادہ عام جرائم میں سے ایک ہے۔ ہیکرز ہمارے WiFi، ای میل اور سوشل میڈیا اکاؤنٹس کے پاس ورڈ Password کو ہیک کر لیتے ہیں۔ ہیکرز ویب سائٹس پر حملہ کر کے اُسے ختم کر دیتے ہیں۔ چنانچہ ہیکنگ کا میدان بہت وسیع ہے۔ ہیکرز حکومتی اور تجارتی آرگنائزیشن کی حساس معلومات کو چرا کر اُس سے فراڈ ٹرانزیکشن Transaction کرتے ہیں اور کوائف کو cloud یا نیٹ ورک کمپیوٹرز پر سب منادیتے ہیں۔

حکومت نے بھی سائبر کرائم کو ختم کرنے کے لیے کچھ طریقے اختیار کیے ہیں۔ خاص طور پر سائبر دھمکیوں اور خوف پھیلانے کے تدارک کے لیے کچھ طریقے بنائے ہیں۔ پاکستان میں نیشنل ریسپانس سینٹر فار فائبر کرائم قائم کیا گیا ہے تاکہ سائبر کرائم کا شکار ہونے والوں کی مدد کی جاسکے۔ آن لائن یا پھر مددگار لائن 9911 پر کال کر کے مدد حاصل کی جاسکتی ہے۔ جو کہ 24/7 سے موجود ہے۔

- کمپیوٹر وائرس کی تعریف کیجئے اور بتائیے کہ اُن سے بچاؤ کس طرح سے کیا جائے۔
- مختلف اقسام کے وائرس کی تعریف کیجئے: Virus, malware, worm, spyware and adware اور مختلف طریقوں سے پھیل سکتا ہے۔
- اس بات کو پہچانیں یا تسلیم کریں کہ اینٹی وائرس سوفٹ ویئر جیسا کہ Norton, Avast, Mac Afee اور دیگر وائرسز کے خلاف تحفظ فراہم کر سکتی ہیں۔



5.2 MALWARE مال ویئر:

Malware کی اصطلاح پُر آزار سوفٹ ویئر کا سکڑاؤ ہے۔ Malware ایک وسیع اصطلاح ہے جو کہ کمپیوٹر وائرس، وائرسز، اسپائی ویئر، adware اور دیگر کے گرد گھیرا ڈال کر حملے سے بچاؤ کرتی ہے۔ Malware وہ پروگرام ہے جو عام طور پر اس لیے لکھی جاتی ہے کہ افرا تفری پھیل جائے۔ یہ اتنے خطرناک ہوتے ہیں کہ یہ ڈوائسز کو بھی تباہ کر سکتے ہیں۔ پس عام طور پر Malware کوائف کو توڑ پھوڑ دیتی ہے، چرالیتی ہے یا delete کر دیتی ہے۔ یانبیادی کاموں کو ہائی جیک کر لیتی ہے اور مختلف سرگرمیوں کو ڈسٹرب کر دیتی ہے

5.2.1 مختلف مال ویئر (Malware):

مال ویئر کی اقسام میں کمپیوٹر وائرسز، وارمز، adware اور اسپائی ویئر شامل ہیں۔

(i) کمپیوٹر وائرس

کمپیوٹر وائرس کمپیوٹر کا پروگرام ہے جو کمپیوٹروں اور اُن کے نیٹ ورک میں اپنے جیسی نقول بنا کر پھیل سکتا ہے۔ عام طور پر استعمال کرنے والے کے علم میں آئے بغیر یہ دوسرے کمپیوٹر پروگراموں میں تبدیلی لاسکتا ہے۔ اپنا ذاتی کوڈ وہاں ڈال کر کمپیوٹر کی

کمپیوٹر کو نئے نئے استعمال کرنے والوں کو نشانہ بناتے ہیں کہ وہ اُس لنک پر کلک کریں جہاں غلط قسم کی malware ہے یا پھر اپنی سوشل میڈیا کی سائنس کے ذریعے ذاتی معلومات فراہم کرنے کی چال چلتے ہیں۔

(v) سائبر دھمکیاں یا ہراساں کرنا

برقی ذرائع جیسا کہ کمپیوٹر، موبائل فون یا انٹرنیٹ بھی آن لائن دھمکیوں یا ہراساں کرنے کے لیے استعمال کیے جاتے ہیں۔ نقصان دہ دھمکیوں والے رویوں میں افواہیں، دھمکیاں، نامناسب فقرے کرنا، ذاتی معلومات کو افشاء کرنا، بلیک میل کرنا اور نفرت بھری تقریر کرنا شامل ہیں۔ ایسا کرنے والے کا مقصد نشانہ بنائے گئے شخص کو نقصان پہنچانا ہوتا ہے۔ نشانہ بننے والا/والی کی خود اعتمادی کم ہو جاتی ہے جسکی وجہ سے وہ خود کشی تک کر سکتا/کر سکتی ہے اور کئی قسم کے منفی جذباتی رد عمل کا شکار ہوتا/ہوتی ہے جس میں خوفزدہ ہونا، مایوسی کا شکار ہونا، غصہ ہونا اور اسی اور غمگین رہنا شامل ہیں۔

5.1.4 سائبر حملہ

سائبر حملہ اُس وقت ہوتا ہے جب سائبر مجرم کمپیوٹر یا کسی اور مشین کے ذریعے اکیلے یا کئی کمپیوٹر نیٹ ورک پر کرہنگ اسکیم لنک، فیسگ یا کسی اور طریقے سے کمپیوٹر نیٹ ورک پر حملہ کرتے ہیں۔ عام طور پر سائبر حملے کوئی فائدہ حاصل کرنے کیلئے یا پھر اپنے شکار کو یا کمپیوٹر، نیٹ ورک یا ویب سائٹ کو نقصان پہنچانے کے لئے کرتے ہیں۔ سائبر حملہ یا تو نشانہ بنائے جانے والے کمپیوٹر کو کام کرنے کے قابل نہیں چھوڑتا یا معلومات کو وہاں سے ختم کر دیتا ہے یا پھر اسے Offline ہونے پر کھٹکھٹاتا (knocks if offline) ہے۔ یہ کمپیوٹر یا نیٹ ورک سے متعلق معلومات کو بھی دہرا لیتا ہے۔

5.1.4 اگر ہم اس کا شکار ہو جاتیں تو ہمیں کیا کرنا چاہیئے؟



Cyber کرائم کرنے والا ہمیشہ یہ کہے گا کہ اس کا رابطہ خفیہ رکھا جائے۔ بصورت دیگر شکار ہونے والا بہت بھاری نقصان اٹھائے گا۔ سافٹویئر کرائم کا شکار ہونے والے کا رد عمل دھمکیاں دینا یا خوف پھیلانا بہت اہمیت کا حامل ہے اس قسم کے پُر آزر افراد لوگوں سے نجات کے کچھ طریقے ہیں۔ سب سے پہلے ان واقعات کو کچھ قابل بھروسہ لوگوں کو بتانا ہو گا جو کہ والدین اور اساتذہ ہو سکتے ہیں۔

شکل 5.1 سائبر ریکوری ہیلپ لائن

سوفٹ ویئر کو اسکی ٹرمز اور کنڈیشنز کو پڑھے بغیر اپنے کمپیوٹر پر انسٹال کر لیتے ہیں۔ سسٹم مانیٹرز، کوئیز ٹریکرز، روٹ کٹس، اور Key loggers، اسپائی ویئر کی چند مثالیں ہیں۔

5.2.2 وائرس کے پھیلنے کے طریقے

کمپیوٹر کا وائرس بالکل اسی طرح کا وائرس ہے جیسا کہ فلو کا وائرس۔ یہ ایک مشین سے دوسری مشین میں پھیلنے کے لیے بنایا گیا ہے۔ اور یہ اپنے آپ کی نقل بنا سکتا ہے۔ کوئی بھی ڈیوائس جس میں وائرس کی انفیکشن ہو وہ دوسری ڈیوائس میں وائرس کو پھیلا سکتی ہے۔ اس کا مطلب یہ ہے کہ وائرس باہر سے آتے ہیں۔ یہ کیسے آتے ہیں؟ یہاں چند طریقے دیئے گئے ہیں۔

(i) USB فلش ڈسک اور CD

USB فلش ڈسک سب سے عام ذریعہ ہے جو فائلز کو منتقل کرتا ہے۔ انفیکٹڈ کمپیوٹر وائرس کو ایسی صاف USB فلش ڈرائیو میں پھیلا سکتی ہے جسے کمپیوٹر میں لگایا گیا ہو اور بالکل اسی طرح سے انفیکٹڈ USB وائرس کو کمپیوٹر میں منتقل کر سکتی ہے۔ ونڈوز میں OS آٹورن فنکشن، CD یا فلش ڈرائیو کے لگانے پر ونڈوز میں موجود آٹورن فنکشن OS اور دوسرے پروگرام خود بہ خود فلش ڈرائیو یا CD کو کمپیوٹر میں لگانے پر انسٹالرز اور دوسرے پروگرامز کو لاؤنچ کر دیتا ہے۔ USB۔CD سے انفیکٹڈ فائلز کو منتقل کرنے سے کمپیوٹر بھی انفیکٹڈ ہو جاتا ہے

اساتذہ وائرسز کی معلومات طلباء کو فراہم کریں جیسا کہ Trojan horses Root kit, Back door

اور Boots۔ یہ ایک اسائنمنٹ کے طور پر بھی دیا جاسکتا ہے۔

اساتذہ کے لیے نوٹ:-



(ii) انٹرنیٹ ڈاؤن لوڈز

کمپیوٹر کے وائرس فائلز یا انٹرنیٹ سے سوفٹ ویئر ڈاؤن لوڈز کے ذریعے بھی پھیلتے ہیں۔ یہ سوفٹ ویئر یا ان فائلز سے جڑے ہوتے ہیں جنہیں ہم ڈاؤن لوڈ کرتے ہیں۔ وائرس جو انٹرنیٹ سے آتے ہیں وہ ہمارے کمپیوٹر تک ہیکرز کی رسائی کر دیتے ہیں۔ حالانکہ تقریباً ہر اینٹی وائرس سوفٹ ویئر ضرور ضرر رساں ڈاؤن لوڈ کیلئے ایک حفاظتی شیلڈ بن جاتی ہے۔ اس بات کی بہت زیادہ ہدایت کی جاتی ہے کہ فائلز کو ہمیشہ قابل بھروسہ ذرائع سے ڈاؤن لوڈ کیا جائے۔

سینک کو تبدیل کر دیتا ہے۔ وائر سز نقصان دہ ہوتے ہیں۔ یہ ناقابل برداشت پیغامات دکھا کر تمام دستاویز تک رسائی کرتے ہیں یا یہاں تک کہ انہیں وہاں سے مٹا دیتے یا غائب کر دیتے ہیں۔ وائر سز عام طور پر میزبان کی فائل پر جاتے ہیں اور جب وہ وہاں پہنچتے ہیں تو وہ دوسری فائلز کو بھی یا پھر وگرا مز کو infect کر دیتے ہیں۔ Boot سکٹر، ریسٹورنٹ، میکرو وائر سز اور فائل انفیکٹر وائر سز کی چند مثالیں ہیں۔

(ii) وائر م

کمپیوٹر کا وائر م اپنی نقل کو کمپیوٹر سے کمپیوٹر تک پھیلا دیتا ہے۔ وائر م کسی بھی انسانی رابطے کے بغیر اپنے نقول بنا سکتا ہے۔ ایسے نقصان پہنچانے کے لیے اپنے آپ کو کسی فائل سے منسلک کرنے کی ضرورت نہیں ہوتی۔ یہ آزار پہنچانے کی نیت سے کئی کام کر سکتا ہے جیسا کہ دوسری malware کو ڈراپ کرنا۔ اپنے آپ کی نقل ڈیوائس میں کر دینا۔ طبعی طور پر متاثرہ نظام سے جڑے رہنا۔ فائلز کو اڑا (delete) کر دینا اور اندرونی اسٹوریج اور یادداشت کے ذرائع کو خراج کر دینا۔

(iii) ایڈویئر

ایڈویئر اشتہارات کو سپورٹ کرنے والی سوفٹ ویئر ہے۔ یہ نہ ختم ہونے والے اشتہارات اور popup ونڈوز جس میں یادداشت اور یادداشت کے ذرائع کو خراج کرنے کی صلاحیت ہے۔ ایڈویئر انٹرنیٹ براؤزر کی مختلف سینک کو جیسا کہ ہوم پیج اور ڈی فالٹ سرچ انجن کو بھی تبدیل کرنے کی صلاحیت رکھتی ہے۔ پس ایڈویئر استعمال کرنے والے کو پریشان کرتی ہے اور پروسینگ کو آہستہ کر دیتی ہے۔ Adware کے بنائے ہوئے اشتہارات بعض اوقات popup کی شکل میں ہوتے ہیں یا پھر بعض دفعہ چھوٹی ونڈوز میں ہوتے ہیں جسے بند نہیں کیا جاسکتا ہے۔ ایڈویئر کے پروگرامز میں کھیل، ڈیکس ٹاپ ٹول بارز اور یوٹیلیٹیز شامل ہیں۔ عام طور پر ایڈویئر ویب بیڈ ہوتی ہے اور ویب براؤزر کے کوائف کو جمع کر کے اشتہارات کو نشانہ بناتی ہے۔ خاص طور پر Popups کو۔

(iv) اسپائی ویئر

اسپائی ویئر ایک malware ہے جو ڈیوائس کو مانیٹر کر کے کسی بھی شخص یا آرگنائزیشن کے بارے میں ان کی مرضی کے بغیر معلومات کو چرا کر اُسے کسی دوسرے شخص یا آرگنائزیشن کو دے دیتی ہے۔ اسپائی ویئر موبائل فون یا کمپیوٹر سے استعمال کرنے والے کی مرضی کے بغیر کنٹرول کی جاتی ہے۔ یہ ایسی معلومات جیسا کہ ویب براؤزنگ کی تاریخ، ای میل کے پیغامات استعمال کرنے والے کا نام، پاس ورڈ اور آن لائن خریداری کی معلومات کو حاصل کر لیتی ہے۔ اسپائی ویئر کو کیلرز کے ذریعے یا پھر اُس وقت جب ہم

والے کو ہوشیار کرتی ہے اور انفیکٹڈ فائلز کو quarantine کرنے کا کہتی ہے۔ اس بات کی بہت زیادہ تاکید کی جاتی ہے کہ استعمال کرنے والا اینٹی وائرس کو پابندی سے update کرے۔ کئی اینٹی وائرس سوفٹ ویئر انٹرنیٹ پر مل سکتی ہیں اور ان میں سے زیادہ تر مفت ہیں۔ پس اینٹی وائرس کے مفت ورژن میں کچھ ترقی یافتہ خصوصیات موجود ہیں۔ پیسے دینے والے خریدار جنہیں پر پریکٹس یوزر کہتے ہیں انہیں ترقی یافتہ حفاظتی خصوصیات مل جاتی ہے۔

سب سے زیادہ عام اینٹی وائرس یہ ہیں:

Avast(i)



شکل 5.3 Avast اینٹی وائرس

Avast دنیا میں سب سے بڑی حفاظتی کمپنیوں میں سے ایک کمپنی ہے Avast کی انتظامیہ یہ دعویٰ کرتی ہے کہ وہ next-gentechology ٹیکنالوجی ساہر حملوں سے لڑنے کے لیے اسی وقت استعمال کرتی ہے۔ وہ یہ بھی دعویٰ کرتے ہیں کہ Avast ایک زبردست اور لامحدود بادلوں پر قائم کی گئی مشینوں سے آموزشی انجن ہے جو مسلسل ہزاروں لاکھوں استعمال کرنے والوں کے کوائف کو مسلسل لہروں کی شکل میں وصول کرتا رہتا ہے۔ یہ آموزشی کی غیر معمولی رفتار سے سہولت کاری کرتا ہے اور مصنوعی ذہانت کے انجن کو وائرس کو رکھنے کے لیے بہت تیز اور اسمارٹ بنا دیتا ہے۔

شکل 5.3 Avast اینٹی وائرس

Norton(ii)



شکل 5.4 Norton اینٹی وائرس

Norton 1991ء سے بہت مقبول اینٹی وائرس سہولت ہے۔ یہ سیکیورٹی کرنے والے وسیع خاندان اور Symantec کارپوریشن کی دیگر سہولتوں کا حصہ ہے۔ Norton اینٹی وائرس باآسانی استعمال کیا جاسکتا ہے۔ اس میں ترجیح دینے کا اختیار ہوتا ہے جسے ماہرین استعمال کر سکتے ہیں۔ اسے ٹیسٹ کرنے والی لیبارٹریز سب سے اعلیٰ مقام پر رکھتی ہیں اور یہ اس طرح سے ڈیزائن کیا گیا ہے کہ یہ آپ کے سسٹم کی کارکردگی پر بہت کم ممکنہ اثر ڈالتا ہے۔

(iii) کمپیوٹر نیٹ ورک

استعمال کرنے والے کو محتاط رہنا چاہیے کیونکہ مقامی علاقے کے نیٹ ورک (LAN) سے لی گئی فائلیں انفیکٹڈ ہو سکتی ہیں اور ہمارے کمپیوٹر یا آپریٹنگ سسٹم کو نقصان پہنچا سکتی ہیں۔ ایسا ہی ایک موبائل سے دوسری موبائل ڈیوائسز میں بلیو ٹوتھ وغیرہ کے ذریعے فائلز کی منتقلی کرنے میں ہو سکتا ہے۔

(iv) ای۔ میل ایچیمینٹس



شکل 5.2 وائرس ای میل
کے ذریعے پھیل سکتا ہے

ای میل ایچیمینٹس وائرس کے پھلاؤ میں سب سے زیادہ مشہور ذریعہ ہے۔ وائرسز ایک کمپیوٹر سے دوسرے کمپیوٹر میں ای میل ایچیمینٹ کے ذریعے منتقل ہو سکتے ہیں۔ انفیکٹڈ میلز اجنبی یا جعلی ای میل پتے سے آ سکتی ہیں۔ وہ مجرم جو ان وائرسز کو پھیلاتے ہیں یا تو جعلی ای میل پتہ استعمال کرتے ہیں یا ایک قابل اعتبار ای میل ایڈریس کے چند حروف تبدیل کر دیتے ہیں۔ ہماری کونٹیکٹ لسٹ میں موجود لوگ بھی ہمیں انفیکٹڈ فائلز بھیج سکتے ہیں کیونکہ وہ خود بھی اس بات سے آگاہ نہیں ہوتے۔ استعمال کرنے والے کو ای میل کا Origin فائلز کو کھولنے سے پہلے یا کسی بھی لنک پر کلک کرنے سے پہلے چیک کرنا چاہیے خاص طور پر spam میلز کو ان کے ایچیمینٹ پر کلک کرنے سے پہلے چیک کرنا چاہیے۔

5.2.3 اینٹی وائرس

اینٹی وائرس ہویٹیلیٹ سو فٹ ویئر ہیں جنہیں کوائف یا بارڈ ویئر کے نقصان سے بچنے کے لیے کسی طرح کی ممکنہ دھمکیوں سے محفوظ رکھنے کے لیے بنایا گیا ہے۔ اس بات کی بہت زیادہ سفارش کی جاتی ہے کہ کمپیوٹر استعمال کرنے والا آپریٹنگ سسٹم پر اینٹی وائرس کو انسٹال کر لے۔ جیسا کہ ونڈوز اینٹی وائرس سو فٹ ویئر بیک گراؤنڈ میں کام کرتی ہے اور اس پر سو فٹ ویئر کو مانیٹر کرتی ہے۔ جو اس پر چل رہی ہوتی ہے اور ای میلز یا انٹرنیٹ سے آنے والے کوائف کو بھی مانیٹر کرتی ہے۔ کسی بھی مشکوک سرگرمی کے نتیجے میں ایسی وائرس استعمال کرنے والے کو ہوشیار کرتی ہے اور عمل کرنے کے لیے کہتی ہے۔ عام طور پر اینٹی وائرس استعمال کرنے

- اپنے spam بلاکنگ یا فلٹرنگ ٹولز کو استعمال کر کے فوری پیغامات اور popups کے ذریعے unsolicited ای میلز کو بلاک کریں۔
- انٹرنیٹ پر موجود قابل بھروسہ ذریعے سے حاصل ہونے والی فائلز اور پروگرام ڈاؤن لوڈ کریں۔
- کبھی بھی WiFi کو نہ کھولیں اور نہ استعمال کریں۔

5.2.5 کوائف کا معیار رکھنا:

- ہمیں کسی بھی ممکنہ نقصان سے بچنے کے لیے کچھ احتیاطیں کرنی ہوں گی۔ اس سلسلے میں چند اقدامات یہ ہیں۔
- پابندی سے سسٹم ری اسٹور پوائنٹ بنائیں اور چیک کرتے رہیں کہ یہ ناکارہ تو نہیں ہو گیا ہے۔
- CD یا DVD پر اہم کوائف لکھیں کیونکہ یہ لکھے ہوئے یا تحریر کیئے ہوئے کوائف محفوظ ہیں اور وائرس سے متاثر نہیں ہوتے۔
- اپنی فائلوں کا بیک اپ ایک سے زیادہ جگہوں پر رکھیں۔
- آپ اپنے مسودے، cloud اسٹوریج جیسا کہ گوگل ڈرائیو اور مائکروسوفٹ ون ڈرائیو پر بھی save کر سکتے ہیں۔

Authentication میکانزم کو بیان کیجئے

- مختلف Authentication میکانزم کی فہرست بنائیں
- کمپیوٹر استعمال کرنے والے کے نام، پاس ورڈ ذاتی شناخت کے نمبر اور بائیو میٹرک Authentication میکانزم کے درمیان تفریق کیجئے



5.3 Authentication میکانزم

آئینٹیکیشن میکانزم، ہارڈ ویئر یا سوفٹ ویئر کا وہ میکانزم ہے جو استعمال کرنے والے کو اس بات پر مجبور کرتا ہے کہ وہ ڈیوائس پر موجود data یا کوائف تک رسائی سے پہلے اپنی شناخت کرائیں۔ اس عمل سے یہ بات یقینی ہو جاتی ہے کہ صرف اصلی یا حقیقی استعمال کرنے والے ہی کوائف یا ڈیوائس تک رسائی کر سکیں۔



شکل 5.5 McAfee اینٹی وائرس

MAC Afee(iii)

MAC Afee یہ دعویٰ کرتا ہے کہ وہ ہیک وقت اینٹی وائرس، پرائیوسی اور شناختی ٹولز اور خصوصیات مہیا کرتا ہے۔ یہ استعمال کرنے والے کو سب سے بعد میں (latest) آنے والے وائرس spyware، ransomware، malware کے حملے سے محفوظ رکھتا ہے جبکہ اُن کی ذاتی شناخت اور پرائیوسی بھی محفوظ رہتی ہے۔

5.2.4 Malware کے خلاف حفاظت

ہمیں اپنے آپ کی حفاظت Malware اور وائرس سے کرنا ہمارے اپنے ہاتھ میں ہے۔ نوے فیصد سے زیادہ کمپیوٹرز میں انفیکشن کمپیوٹر استعمال کرنے والے کی غلطی سے ہوتی ہے۔ ہمارے کمپیوٹر میں وائرس اُس وقت آتا ہے جب وہ آہستہ ہونے لگتے ہیں، خلاف معمول رد عمل ظاہر کرتے ہیں (ٹھیک نہیں چلتے) کام کرنے کے دوران کریش ہو جاتے ہیں یا پھر کئی مرتبہ دوبارہ اسٹارٹ ہوتے ہیں۔ مسلسل تنگ یا پریشان کرنے والے پیغامات بھیجتے ہیں یا ہمارے کچھ مسودے غائب ہو جاتے ہیں یا پھر اُن تک ہماری پہنچ نہیں ہو سکتی۔ ہمیں ایسے حالات پیدا ہونے سے بچنا چاہیئے۔ بعض سادہ احتیاطیں ہمارے سسٹم کو Malware اور وائرس سے بچا سکتی ہیں۔

- اینٹی وائرس سوفٹ ویئر کو کمپیوٹر میں انسٹال کر دیں اور اُسے اپ ڈیٹ کرتے ہیں۔
- اپنی اینٹی وائرس سوفٹ ویئر کو شیڈیول کے مطابق پابندی سے چلائیں۔
- اپنے آپریٹنگ سسٹم کو update رکھیں۔
- غیر معمولی لیبل، تصاویر یا Captions والے انٹرنیٹ لنکس پر کلک نہ کریں۔
- ای میل ایٹچمنٹ کو نہ کھولیں یا بغیر جان پہچان والے ای میل بھیجنے والوں کی ای میل مت کھولیں۔
- USB فلپش ڈسک، SD کارڈز اور موبائل فونز کو کھولنے سے پہلے اسکین کریں۔



شکل 5.6 شیڈول اینٹی وائرس اسکین
ڈیٹا کو محفوظ رکھ سکتا ہے۔



شکل 5.8 آئرس کا اسکین اور انگلیوں کے نشان

میٹرک کوائف اُس سے مل جاتے ہیں تو پھر اس بات کی تصدیق ہو جاتی ہے کہ یہ درست ہیں۔ انگلیوں کے نشان کو اسکین کرنا بائیو میٹرک کا سب سے عام طریقہ ہے۔ لیکن بعض زیادہ ترقی یافتہ طریقوں میں ریٹینا کا اور Iris کا اسکین، چہرے اور آواز کی شناخت ہے۔

- کمپیوٹر کے میدان میں پیشہ ورانہ اخلاقیات کی اہمیت بیان کیجیئے۔
- معلومات کی درستی کی تعریف بیان کیجیئے۔
- مختلف اقسام کے انٹیلیجنس، پراپرٹی حقوق، patent، کاپی رائٹس اور ٹریڈ مارکس کی وضاحت کیجیئے۔
- سوفٹ ویئر کی پرائیوسی اور اُس کے اثرات کی وضاحت کیجیئے۔
- معلومات کی پرائیوسی کو بیان کیجیئے۔
- Plagiarizer پر گفتگو کیجیئے۔

مقاصد خاص

SLO

5.4 کمپیوٹر کے میدان میں پیشہ ورانہ اخلاقیات

پیشہ ورانہ اخلاقیات میں ذاتی اور کارپوریٹ اصول اور رولز ہوتے ہیں جو پیشے کے اعتبار سے ہمارے کردار کی رہنمائی کرتے ہیں۔ پیشہ ورانہ اخلاقیات کا کوڈ ویلیوز اور رولز کی وضاحت کرتا ہے اور ڈسپلین کے لیے ڈھانچے کے طور پر استعمال کیا جاسکتا ہے کمپیوٹر کے پیسہ ورانہ ماہرین دنیا کو تبدیل کر سکتے ہیں۔ پیشہ ورانہ اخلاقیات کا کوڈ اقدار اور قوانین کی وضاحت کرتا ہے اور ڈسپلین کے لیے ڈھانچے کے طور پر استعمال کیا جاسکتا ہے۔ ذمہ دارانہ طور پر عمل کرنے کے لیے انہیں اپنے کام کے وسیع اثرات پر عکاسی کرنی چاہیئے مستقل طور پر پبلک کی چیزوں کو سپورٹ کرنا چاہیئے۔ یہاں کچھ رہنما اصول دیئے گئے ہیں۔

- سوسائٹی اور انسانیت کی بھلائی کے لیے کام کریں اور اس بات کا اعتراف کریں کہ کمپیوٹر میں لوک اسٹیک ہولڈر ہیں۔
- ایماندار اور قابل بھروسہ رہیں۔

5.3.1 محفوظ رکھنے کے طریقوں کی اقسام

بہت سارے ایسے طریقے ہیں جن کے ذریعے کمپیوٹر کی حفاظت ہوتی ہے۔ اور اصلی استعمال کرنے والا ہی اسے استعمال کر سکتا ہے۔ ان طریقوں میں سے چند یہ ہیں۔

(i) استعمال کرنے والے کا نام اور پاس ورڈ

استعمال کرنے والے کا نام اور پاس ورڈ کمپیوٹر کھولنے والے لفظوں کا وہ جوڑا ہے جو صرف استعمال کرنے والے کو پتہ ہوتا ہے۔ یہ کمپیوٹر میں محفوظ کیا جاتا ہے تاکہ وہ باختیار استعمال کرنے والے کو پہچان لے۔ استعمال کرنے والے کا نام اور پاس ورڈ کی فالٹ Authentication میکانزم ہے جو آجکل web پر دستیاب ہے۔ بس نئے وسیع پیمانے کے کمپیوٹر حملے نے استعمال کرنے والے کا نام اور پاس ورڈ کو ناقابل حقیقت کی تصدیق کرنے والے میکانزم بنا دیا ہے۔ اضافی تصدیق کے میکانزم کی مکمل طور پر تصدیق کے لیے ضرورت ہوتی ہے۔

(ii) ذاتی شناخت کا نمبر



PIN ذاتی شناخت کے نمبر کو ظاہر کرتا ہے۔ یہ حفاظت کا کوڈ

ہے جو آپ کی شناخت کی تصدیق کرتا ہے۔ پاس ورڈ کی طرح آپ کا پین نمبر بھی آپ کو خفیہ رکھنا چاہیے کیونکہ یہ اہم خدمات کی اجازت دیتا ہے جیسا کہ مالی کاروباری امور کی انجام دہی اور خفیہ ای میل PIN حفاظت کرتا ہے جب کریڈٹ / ڈیبٹ کارڈ بھی کھوجانا یا چوری ہو جاتا ہے کیونکہ PIN کا جاننا پیسے نکالنے یا ٹرانسفر کرنے کے لیے ضروری ہوتا ہے۔

فصل 5.7 PIN ذاتی شناخت

(iii) بائیومیٹرک تصدیق

Authentication کے عمل کے برخلاف، بائیومیٹرک اس بات کو یقینی بناتی ہے کہ اصلی شخص ہی کوائف یا پھر ڈیوائس تک رسائی حاصل کرے، بائیومیٹرک تصدیق اس شخص کی یکتا حیاتیاتی خصوصیات پھر بھروسہ کرتی ہے۔ بائیومیٹرک تصدیقی نظام اسی وقت (حقیقی وقت) میں کوائف کو لیکر ڈیٹا بیس (data base) میں موجود ڈیٹا سے موازنہ کرتا ہے۔ اگر بائیو

بھروسہ ذرائع کے استعمال کے نتیجے میں غلط معلومات حاصل ہو گئی۔ خاص طور پر معلومات کی سوشل میڈیا پر بتائی گئی معلومات اکثر سوالیہ نشان ہوتی ہیں۔

5.4.2 انٹیلیکچوئل پراپرٹی رائٹس

جب کوئی شخص سوفٹ ویئر بناتا ہے، کتاب لکھتا ہے یا تحقیقی مقالہ یا کسی بھی طریقے کو یا مشین کو ایجاد کرتا ہے تو یہ اُس شخص کی انٹیلیکچوئل ملکیت ہو جاتی ہے۔ انٹیلیکچوئل پراپرٹی انسانی ذہانت کی ناقابل گرفت پراپرٹی یا ملکیت ہے جسے چرایا بھی جاسکتا ہے اسے چوری سے بچانے یا غیر قانونی استعمال سے بچانے یا اس کے غیر قانونی استعمال سے بچنے کے لیے انٹیلیکچوئل ملکیت کے حقوق پر عمل کیا جاتا ہے ان حقوق کے ذریعے انٹیلیکچوئل ملکیت کو کاپی رائٹ، پیٹنٹ اور ٹریڈ مارک کے ذریعے محفوظ کیا جاتا ہے۔ اسکی وجہ سے تخلیق کرنے والے یا پیٹنٹ کے، ٹریڈ مارک یا کاپی رائٹڈ کام کرنے والوں کو اپنے کام سے فائدہ حاصل ہوتا ہے یا



شکل 5.10 انٹیلیکچوئل ملکیت کے پراپرٹی حقوق کا خیال رکھیں

انویسٹمنٹ حاصل ہوتی ہے۔ ان حقوق کے تحت کوئی دوسرا فرد یا آرگنائزیشن کسی دوسرے کی انٹیلیکچوئل پراپرٹی کی نقل تو کر سکتا ہے اور نہ ہی اس کی نقل تیار کر سکتا ہے۔ انٹیلیکچوئل پراپرٹی کے حقوق پوری دنیا میں تسلیم کیے جاتے ہیں۔ پاکستان میں انٹیلیکچوئل ملکیت کی آرگنائزیشن (IPO) انٹیلیکچوئل پراپرٹی رائٹس (انٹیلیکچوئل ملکیت کے حقوق کو کنٹرول کرتی ہے۔)

(i) پیٹنٹ



شکل 5.11 پیٹنٹ

پیٹنٹ Exclusive یعنی بلا شرکت غیرے کسی بھی ایجاد کو محدود وقت میں بنا کر استعمال کرنے اور بیچنے کے لیے، پاکستان میں 20 سال تک کے لیے ایجاد ہے۔ پیٹنٹ کو رکھنے والے کو یہ حقوق حاصل ہو جاتے ہیں کہ وہ کسی دوسرے کو اجازت کے بغیر اپنی ایجاد کو بنایا بیچ نہیں سکتا۔ طالب علموں اور اسکالرز کی حفاظت کے لیے ہائر ایجوکیشن کمیشن اس بات کی سپورٹ کرتا ہے کہ پیٹنٹ کو انٹیلیکچوئل

- اوزاروں کی عزت کریں۔
 - کی قسم کا نقصان پہنچانے سے گزیر کریں۔
 - سب سے یکساں سلوک کریں اور تعریف، مذاق اڑائیں یا پریشان نہ کریں۔
 - جس کام کی ضرورت ہو اُس کی عزت کریں تاکہ نئے آئیڈیاز، ایجادات اور تخلیقی کام اور کمپیوٹر کے واضح عمل جنم لے سکیں۔
 - پرائیوسی کی عزت کریں اور رازداری رکھیں۔
 - پیشہ ورانہ مقابلے کے لیے اعلیٰ معیار رکھیں اور اخلاقی کام کریں۔
 - دوسرے افراد یا گروہ کے لیے پیشہ ورانہ اہلیت، صلاحیت یا استعداد اور اخلاقی اعمال پر قائم رہیں۔
 - اعلیٰ درجے کے پیشہ ورانہ معیارات قائم رکھیں۔ اخلاقی کام کریں۔
 - اس بات کو یقینی بنائیں کہ افراد اور ذرائع کام کرنے کی زندگی کی کوالٹی میں اضافے کے لیے ہیں۔
 - جب آپ کو کمپیوٹنگ اور ذرائع ابلاغ کے ریسپوسز کو استعمال کرنے کی اجازت ہو تب ہی استعمال کریں۔
 - پبلک کو کمپیوٹنگ سے آگاہ کریں اور کمپیوٹنگ کو سمجھائیں اور اس سے متعلق ٹیکنالوجی اور اُن کے نتائج سے آگاہ کریں۔
- 5.4.1 معلومات کی درستگی کی تعریف بیان کریں۔**



شکل 5.9 معلومات کی درستگی

معلومات کی درستگی اس قسم کی پیمائش ہے جو اس بات کو یقینی بناتی ہے کہ معلومات درست اور بالکل صحیح ہیں یہ بھی ضروری ہے کہ معلومات ضرر رساں اور دل آزار کوائف سے نہ حاصل کی گئی ہوں۔ معلومات کی درستگی کے لیے کوائف کو ایک نیک نام اور معزز ذریعے سے حاصل ہونا چاہیے۔

معلومات میں تیزی سے اضافے کے دور میں جب ہم معلومات کا استعمال کریں یا پھر معلومات کو رد کریں تو ہمیں بہت زیادہ محتاط ہونے کی ضرورت ہے۔ ناقابل

5.4.3 سوفٹ ویئر کی (خلاف ورزی) Piracy

سوفٹ ویئر کی خلاف ورزی اُس کا غیر قانونی استعمال، اُس کی نقل کرنا یا پھر کاپی رائٹڈ سوفٹ ویئر کو تقسیم کرنا ہے۔ سوفٹ ویئر کی خلاف ورزی سوفٹ ویئر کی صنعت کے لیے بہت بڑا خطرہ ہے۔ یہ بنانے والوں اور بیچنے والوں دونوں کو ریونیو کا کافی نقصان پہنچاتا ہے۔ نقل کرنے کی وجہ سے بیچنے والوں کے پاس صرف چند ذرائع باقی رہ جاتے ہیں جن کے ذریعے وہ نئی پروڈکٹس کو تلاش کر کے نئی پروڈکٹ کو ڈیولپ کریں۔ کیونکہ انہیں بہت کم نفع ملتا ہے۔ اس لیے انہیں یہ قیمت اپنے خریداروں کو منتقل کرنی پڑتی ہے۔

سوفٹ ویئر کی کمپنیوں نے بہت سی ٹیکنیک استعمال کی ہیں۔ تاکہ سوفٹ ویئر کی نقل تیار نہ ہو سکیں۔ اُن میں سے زیادہ تر کامیاب نہیں ہوئیں۔ یہ کاپی کی حفاظت کے لیے کی گئیں جو استعمال کرنے والے کو مختلف Keys چابیاں Enter کرنے کا کہتی ہیں، آجکل زیادہ تر سوفٹ ویئر میں رجسٹریشن کی ضرورت ہوتی ہے جو آن لائن ہوتا ہے۔ لیکن ان احتیاطوں نے بھی Piracy کو نہیں روکا۔ Pirated سوفٹ ویئر کو استعمال کرنا استعمال کرنے والے کے لیے بھی risky ہے۔

پائریٹڈ سوفٹ ویئر کے استعمال کرنے کے قانونی نقصانات کے علاوہ استعمال کرنے والا کچھ عملی فوائد بھی کھودیتا ہے۔ نقل شدہ سوفٹ ویئر درست طور پر کام نہیں کر سکتی یا پھر کسی بھی وقت کام کرنا بند کر دیتی ہے۔ اسکے علاوہ Pirated سوفٹ ویئر کا استعمال کرنے والے کو گاہک کی سپورٹ حاصل نہیں ہوتی، اپ گریڈ۔ ٹیکنیکل ڈیویویشن، ٹریننگ اور bug فلکسنگ بھی حاصل نہیں ہوتی۔

Plagiarism 5.4.4

Plagiarism کسی اور کے کام کو یا خیالات کو اُسکے مصنف کے کام کے مکمل اعتراف کے بغیر اپنے نام سے پیش کر دینے کو کہتے ہیں۔ اکیڈمی ایمانداری کا تقاضہ یہ ہے کہ کسی بھی خیال، الفاظ اور data کو استعمال کرنے والا اُس کے اصل خالق کو سراہے۔ اس کی وجہ سے خالق یا پیٹنٹ کو بنانے والا یا ٹریڈ مارک کا خالق یا کاپی رائٹڈ کام کرنے والا اپنے کام یا Investment سے فائدہ پہنچاتا

پراپرٹی آرگنائزیشن (IPO) کے ساتھ رجسٹر کریں۔ پینٹ ایبل پروسیس یا ایجاد کو یکتا، ایجاداتی اقدامات سے بھرپور اور صنعتوں میں استعمال کے قابل ہونا چاہیے۔

(ii) کاپی رائٹس



شکل 5.12 کاپی رائٹس

کاپی رائٹس قانونی ہتھار ہے جو آرٹ ورک، لٹریچر یا معلوماتی پروگرام آرٹ کے کام یا وہ کام جو معلومات فراہم کرتا ہے یا آئیڈیاز دیتا ہے۔ سادہ الفاظ میں کاپی رائٹ میں یہ حق دیتا ہے کہ کام کو کس طرح سے استعمال کیا جائے۔ کاپی رائٹ کا مقصد یہ ہے کہ وہ معلومات کی ترقی کو آگے بڑھائے، کام کے اُس منصف کو مالی فائدے کی ترغیب دے تاکہ وہ نیا کم کرے۔ C کا نشان کاپی رائٹڈ چیزوں پر اکثر لکھا جاتا ہے۔

(iii) ٹریڈ مارک



شکل 5.13
ٹریڈ مارک رجسٹری

کسی پروڈکٹ یا سروس کو شناخت کرتا ہے اور اُسے دوسری پروڈکٹ اور سروسز سے نمایاں یا ممتاز بناتا ہے۔ ٹریڈ مارک انٹیلیکچوئل پراپرٹی رائٹس کے ذریعے محفوظ کیئے جاتے ہیں جو اس بات کی شناخت کرتا ہے کہ پروڈکٹ یا سروس ایک مخصوص آرگنائزیشن سے تعلق رکھتی ہے۔ یہ ایک بآسانی شناخت کیئے جانے والا لفظ، Phrase، لوگوں یا علامات ہوتا ہے جسے اکثر TM (ٹریڈ مارک) کے طور پر ظاہر کیا جاتا ہے۔ ٹریڈ مارک آرگنائزیشن کو اپنی پروڈکٹ اور خدمات کو مقامی یا بین الاقوامی طور پر مارکیٹ کرنے میں مدد دیتی ہے۔ ٹریڈ مارک بنانا ایک تخلیقی کام ہے اور پیشہ ورانہ طور پر کیا جاسکتا ہے۔ ٹریڈ مارک بنانے کے لیے کئی سوفٹ ویئر دستیاب ہیں۔

- Malicious Software malware ایک وسیع اصطلاح ہے جو کمپیوٹر کے دائرہ میں، ویرس، اسپائی ویئر، ایڈ ویئر اور دیگر جنہیں عام طور پر گڑ بڑچانے کے لیے لکھا گیا ہو۔
- وائرس یا malware، USB، فلیش ڈسک اور CDs، انٹرنیٹ ڈاؤن لوڈز کمپیوٹر نیٹ ورک اور ای میل کے attachment سے پھیل سکتی ہے۔
- اینٹی وائرس فائدہ مند سوفٹ ویئر ہیں جنہیں کمپیوٹر کی حفاظت کے لیے بنایا گیا ہے تاکہ کوائف کو جو ممکنہ خطرہ وائرس یا malware سے کوائف کے یا ہارڈ ویئر کے نقصان کا ہواؤس سے بچ سکے۔
- ڈیٹا کی حفاظت کے لیے فائلوں کا بیک اپ ایک سے زیادہ جگہوں پر رکھنا چاہیے۔
- باختیار ہونے کا میکینزم ہارڈ ویئر یا سوفٹ ویئر پر مشتمل وہ میکینزم ہے جو اس بات کو یقینی بناتا ہے کہ صرف باختیار کرنے والے کو ہی کوائف یا ڈیوائس تک رسائی ہو۔
- پیشہ ورانہ اخلاقیات میں ذاتی اور کارپوریٹ اصول شامل ہیں جو پیشے کے اعتبار سے کردار کی رہنمائی کرتے ہیں۔
- معلومات کی درستگی ایک قسم کی پیمائش ہے جس سے معلوم ہوتا ہے کہ اور یقین دہانی ہوتی ہے کہ معلومات درست اور صحیح ہیں۔
- انٹیکچوئل اثاثے انسانی ذہانت کے ناقابل مشاہدہ اثاثے ہیں۔ اپنی انسانی چوری سے بچانے یا غیر قانونی استعمال سے بچانے یا پھر اس انٹیکچوئل اثاثے کو پھیلنے سے بچانے کے لیے انٹیکچوئل اثاثوں کے حقوق لاگو سمجھے جاتے ہیں۔ ان حقوق کے ذریعے اثاثوں کی حفاظت اثاثوں کے حقوق کا پی رائٹ، پینٹ اور ٹریڈ مارک کے ذریعے کی جاتی ہے۔
- سوفٹ ویئر Piracy، نقل کرنا یا کاپی رائٹڈ سوفٹ ویئر کو تقسیم کرنا یا اس کا غیر قانونی استعمال ہوتا ہے۔
- Plagiarism کی دوسرے کے کام یا خیالات کو اس کے مصنف یا پیش کرنے والے کا مکمل اعتراف یا تسلیم کیے بغیر اپنے نام سے پیش کرنا ہے۔

ہے۔ ان حقوق کے تحت کوئی دوسرا شخص یا آرگنائزیشن کسی دوسرے کی انٹیلیکچوئل ملکیت کی نقل یا دوبارہ پیش نہیں کر سکتی، انٹیلیکچوئل پراپرٹی رائٹس کا تمام دنیا میں دعویٰ کیا جاسکتا ہے۔ پاکستان میں انٹیلیکچوئل پراپرٹی آرگنائزیشن (IPO) انٹیلیکچوئل پراپرٹی کی رائٹس کے معاملات کو دیکھتی ہے۔ ایکڈمک آرگنائزیشن Plagiarism کا پتہ لگانے والوں کی خدمات حاصل کرتی ہے۔ سب سے زیادہ استعمال ہونے والی سروس Turinitin ہے۔

خاتمہ

- کمپیوٹر کی حفاظت اس کو ٹوٹنے سے یا۔ اُس کی ہارڈ ویئر کو چوری سے بچانا ہے۔ اس کی سوفٹ ویئر اور اُس پر موجود معلومات کو وائر سز خطرے سے بچانا یا اُس کو بے اختیار لوگوں کے استعمال سے بچانا ہے۔
- سائبر کرائم وہ کرائم یا جرم ہے جو کمپیوٹر اور نیٹ ورک کے ذریعے کیا جاتا ہے۔
- ہیکرز اپنی مہارت کے ذریعے قانون یا ضابطے سے بچنے کی صورت کی شناخت کر کے اُس پر قابو پاتے ہیں۔
- کریکڑوہ لوگ ہوتے ہیں جو اپنی مہارت کے ذریعے دوسرے سسٹم کا غیر قانونی اختیار حاصل کر لیتے ہیں۔
- Phishing وہ طریقہ ہے جس میں جعلی ای میل اور ویب سائٹس کے ذریعے ذاتی معلومات کو اکٹھا کیا جاتا ہے۔
- الیکٹرانک ذرائع جیسا کہ کمپیوٹر، موبائل فون یا انٹرنیٹ کو آن لائن ڈرانے دھمکانے خوفزدہ کرنے کے لیے استعمال کیا جاتا ہے۔
- سائبر حملہ اُس وقت ہوتا ہے جب ایک سائبر مجرم کمپیوٹر یا کسی بھی ڈیوائس کے ذریعے داخل ہوتا ہے یا حملہ کرتا ہے ایک یا کئی کمپیوٹر نیٹ ورک پر۔
- سائبر حملہ یا سائبر ہراسگی اور دھمکیاں دینا بھی سائبر حملے میں شامل ہیں۔
- جس شخص پر سائبر حملہ یا سائبر ہراسگی ہو اُسے چاہیے کہ کسی قابل بھروسہ شخص اور حکومتی یا اختیار اداروں کو اسکی اطلاع دے۔

6. انٹرنیٹ سے جچھ عبارتوں کی نقل کر کے اس کے اصل مصنف کا اعتراف کئے بغیر اپنے مسودے کا حصہ بنالینا مثال ہے۔

(الف) Plagiarism کی (ب) Patent کی غیر قانونی استعمال کی

(ج) معلومات کی چوری Piracy کی (د) کاپی رائٹ کے توڑنے کی

7. کیونکہ Data کو کوئی نقصان نہیں پہنچتی یا اسے چوری نہیں کرتی اس لئے سب سے کم نقصان دہ Malware ہے۔

(الف) وائرس (ب) ایڈوائیر Adware

(ج) اسپائی ویئر Spyware (د) Trojan

8. وہ Malware جو اپنے آپ کی نقل بنالیتی ہے اور جسے فائلوں کے ساتھ جوڑنے کی ضرورت نہیں ہوتی وہ ہے۔

(الف) وائرس (ب) ایڈوائیر Adware

(ج) اسپائی ویئر Spyware (د) وائرس

9. یہ کس وائرس سے پھیلتا ہے۔

(الف) ایمیل ایٹچمنٹ (ب) انٹرنیٹ ڈاؤن لوڈز

(ج) فلسفی ڈسک اور ED: (د) ان سب سے

10. اس لنک کو کلک کریں اور McDonald میں 5 کا واؤچر حاصل کریں۔ یہ مثال ہے:

(الف) Scan کی (ب) Pishing کی

(ج) Click jacking کی (د) ہیکنگ کی

ب. درج ذیل کا جواب دیجئے۔

1. کمپیوٹر کی حفاظت کیوں ضروری ہے؟ کوئی سی تین وجوہات لکھیے۔

2. Cyber Bullying کی ایک مثال سے وضاحت کیجئے۔

3. معلومات کا درست ہونا کیوں ضروری ہے؟

مشقی سوالات



1. درست جواب کا انتخاب کیجئے۔

1. وہ وسیع اصطلاح جو مختلف نقصان پہنچانے والی سوفٹ ویئر کو ظاہر کرتی ہے۔ وہ ہے

(الف) وائرس (ب) میل ویئر Malware

(ج) ایڈ ویئر Adware (د) اسپائی ویئر Spyware

2. باختیار ہونے کا طریقہ کار جو صرف اصل تخلیق کار کو Data تک پہنچنے یا Device کو استعمال کرنے کی اجازت دیتا ہے۔

(الف) استعمال کرنے والے کا نام اور پاس ورڈ (ب) Pin

(ج) بائیومیٹرک (د) اسکلین کوڈ

3. سوفٹ ویئر زیادہ تر محفوظ کی جاتی ہیں۔

(الف) پبلسٹکس کے ذریعے (ب) کاپی رائٹس کے ذریعے

(ج) ٹریڈ مارکس کے ذریعے (د) Logos کے ذریعے

4. کمپیوٹر کے میدان میں پیشہ ورانہ اخلاقیات اہمیت رکھتی ہے کیونکہ:

(الف) یہ قانونی طور پر ضروری ہے (ب) قانون کے توڑنے سے بہت زیادہ جرمانہ لگ سکتا ہے

(ج) یہ مالی فوائد کے لیے ضروری ہے (د) یہ کام کرنے کے ماحول کو صحت مند اور مثبت رکھتی ہے

5. مفت حاصل ہونے والی اینٹی وائرس سوفٹ ویئر اکثر

(الف) تھوڑے عرصے میں ناکارہ ہو جاتی ہے (ب) محدود خدمات فراہم کرتی ہے

(ج) اسے اپ ڈیٹ نہیں کیا جاسکتا (د) اسے خریدنا نہیں جاسکتا

ج. کاملز کو ملائیے۔

ب	نمبر شمار	الف	نمبر شمار
Adware ایڈویئر	ا	کسی اور کے خیالات کو اس کے مصنف کے نام کے بغیر اپنے نام سے پیش کرنا۔	(i)
Cracker کرکیر	ب	ایک اشتہاری سوفٹ ویئر جس میں اشتہارات اور Popup windows وائرُس پھیلانے کے لیے موجود ہوں۔	(ii)
Pin پن	ج	وہ جرم جو کمپیوٹر سسٹم کے ذریعے کیا جائے۔	(iii)
اینٹی وائرُس	د	ایک خفیہ سیکورٹی کوڈ جو استعمال کرنے والے کی شناخت کرتا ہے۔	(iv)
Plagiarism	ه	وہ شخص جو بغیر کسی اختیار کے پاس ورڈ کے بغیر دوسرے کمپیوٹرز میں غیر قانونی طور پر رسائی حاصل کر لیتا ہے۔	(v)
Cyber Crime سائبر کرائم	و	وہ پولیٹیلی سوفٹ ویئر جو کمپیوٹر، مکیوں اور Data کے نقصان سے بچاتی ہیں۔	(vi)

4. Ethical Hacking کیا ہے؟

5. آپ کا ایک دوست Cyber Harassment کا شکار ہو گیا ہے۔ آپ اسے کون سے دو مشورے دیں گے/گی؟

6. ای میل اکاؤنٹ کی ہیکنگ سے بچنے کے لیے کوئی سے دو اقدامات لکھیے۔

7. سوفٹ ویئر بنانے والوں کے لیے سوفٹ ویئر Piaracy کس طرح سے نقصان دہ ہے۔

8. Pishing کی دو مثالیں دیجئے۔

9. انٹلیکچوئل پراپرٹی حقوق کیا ہیں؟

دی گئی کسوٹی کے مطابق درج ذیل میں تفریق کیجئے۔

اسپائی ویئر	ایڈ ویئر	وارم	وائرس	Criteria کسوٹی
				خطرے کی سطح
				یہ کس طرح سے ہوتی ہے؟
				نقصان جو کہ ڈیٹا اور ہارڈ ویئر کو ہو سکتا ہے۔
				کمپیوٹر کی رفتار پر اثر
				بھیجنے کے ذرائع

سرگرمی 4:

اخبار یا انٹرنیٹ پر ایسی کوئی خبر تلاش کریں جس میں سائبر کرائم کے بارے میں خبر ہو خاص طور پر جس میں مجرم پکڑے گئے ہوں اور سزا دی گئی ہو۔

سرگرمی 5:

تھیسس اور ریسرچ پیپر ز عام طور پر ایک ایسے سوفٹ ویئر کے ذریعے چیک کیے جاتے ہیں جس میں انٹرنیٹ پر منحصر Paid Plagiarism detection سروس موجود ہوتی ہیں۔ دوسری مفت آن لائن سروسز جے کے ذریعے طالب علم Plagiarism کو اپنے مسودے میں کر سکیں ان میں سے چند یہ ہیں۔

WWW.Duplichecker.com

WWW.quetext.com

WWW.plagscan.com

کسی بھی موضوع پر ایک مضمون لکھیے اور کچھ عبارت انٹرنیٹ کی ویب سائٹ سے Copy اور Past کریں۔ پھر اپنے مسودے میں Plagiarism کو چیک کیجئے۔

سرگرمیاں



سرگرمی 1:

ایک پوسٹریکزیبیشن کا اہتمام کریں جس کا طالب علم سامعین کو یہ بتائیں کہ کمپیوٹر اور انٹرنیٹ کس طرح سے بہ حفاظت استعمال کرتے ہیں۔ کچھ منتخب عنوانات یہ ہو سکتے ہیں۔

- اپنے کمپیوٹر کو وائرس سسز اور Malware سے کس طرح محفوظ رکھیں۔
- Cyber حملے اور خوفزدگی کو خیر باد کہیں۔
- Piracy اور Pragiarity کو خیر باد کہیں۔
- سائبر کرائم سے کس طرح نمٹیں۔

سرگرمی 2:

کمرہ جماعت میں گفتگو کے دوران طالب علموں کے سامنے یہ صورت حال رکھیں اور گفتگو کریں کہ وہ اس قسم کی صورت حال میں کیا کریں گے اور کیوں کریں گے۔

- آپ کو کسی نے فون کیا ہے۔ فون کرنے والا یہ دعویٰ کر رہا ہے کہ آپ کو ایک بہت بڑا انعام ملا ہے اور اسے آپ تک پہنچانے کے لئے قبل از پے منٹ کی ضرورت ہے۔
- آپ کو ایک فائل ایک بغیر جان پہچان والے ای میل ایڈریس سے ملی ہے جو آپ سے بینک اکاؤنٹ کی تفصیلات یا تعامل کرنے والے کی ID اور پاس ورڈ مانگ رہی ہے۔
- ایک بغیر جان پہچان والی ویب سائٹ پر سر فنگ کے دوران ویب سائٹ یہ ڈیمانڈ کر رہی ہے کہ آپ اپنے کمپیوٹر پر موجود مواد تک رسائی فیس بک یا Gmail اکاؤنٹ کے ذریعے دیں۔

سرگرمی 3:

سر و سسز کی فہرست بنائیں جو اینٹی وائرس مفت میں فراہم نہیں کرتیں۔