یونٹ 11

کمپیوٹر کے استعمال میں اخلاقی، سماجی، اور قانونی خدشات

اس باب کا مطالعہ کرنے کے بعد طلبہ اس قابل ہو جائیں گے وہ:

- روزمرہ کی سرگرمیوں میں کمپیوٹر کو محفوظ طریقے سے اور ذمہ داری سے استعمال کرنے کی اہمیت کو بیان کر سکیں۔
- کمپیوٹر اور آن لائن پلیٹ فارم استعمال کرتے وقت ذاتی معلومات کی حفاظت کیسے کی جائے اس کی وضاحت کر سکیں۔
- حفاظت، کارکردگی، اور مطابقت کے لیے کمپیوٹر ہارڈ ویئر اور سافٹ ویئر کا انتخاب کرتے وقت غور کرنے والے عوامل کی نشاندہی کر سکیں۔
- وضاحت کر سکیں کہ کس طرح صحیح ہارڈ ویئر اور سافٹ ویئر کا انتخاب کمپیوٹر کے مجموعی تجربے کو متاثر کرتا ہے۔
- مضبوط، منفرد پاس ورڈ بنانے اور ان کی اہمیت کی وضاحت کرنے کا طریقہ سمجھ سکیں۔
- باقاعدگی سے سافٹ ویئر اپ ڈیٹس کی ضرورت اور آلہ کی حفاظت کو برقرار رکھنے میں ان کے کردار کی وضاحت کر سکیں۔
- نامعلوم لنکس پر کلک کرنے اور ناقابل اعتماد ذرائع سے فائلوں کو ڈاؤن لوڈ کرنے سے وابستہ ممکنہ خطرات کی نشاندہی کر سکیں۔
- ٹو فیکٹر اتھینٹیکیشن (2FA) کے تصور اور فوائد کی وضاحت کر سکیں۔
- حساس لین دین کے لیے عوامی وائی فائی کے استعمال کے خطرات اور محفوظ نیٹ ورکس کی اہمیت کی وضاحت کر سکیں۔
- عام آن لائن دھوکہ دہی اور فشنگ کی کوششوں کی شناخت کر کے ان سے بچیں کر سکیں۔
- اہم ڈیٹا کو باقاعدگی سے بیک اپ کرنے کی اہمیت کی وضاحت کر سکیں اور ایسا کرنے کے طریقے بیان کر سکیں۔
- سوشل میڈیا، ای میل، کلاؤڈ سروسز، اور آن لائن ایپلیکیشنز پر ذمہ دارانہ رویے کی وضاحت کر سکیں۔
- آن لائن ذاتی معلومات کی حفاظت میں رازداری کی ترتیبات اور ڈیٹا کی حفاظت کے اقدامات کی اہمیت کی وضاحت کر سکیں۔
- انٹلکچوئل پراپرٹی کے حقوق، بشمول کاپی رائٹ، ٹریڈ مارکس، اور پیٹنٹ سے متعلق اخلاقی اور قانونی ذمہ داریوں کی نشاندہی کر سکیں۔
- انٹلکچوئل پراپرٹی کے احترام کی اہمیت اور سافٹ ویئر پائریسی کے مضمرات پر تبادلہ خیال کر سکیں۔
- رازداری کے قوانین اور آن لائن ذاتی معلومات کی حفاظت میں ان کے مقصد کی وضاحت کر سکیں۔
- ذاتی ڈیٹا تک غیر مجاز رسائی کے قانونی نتائج اور صارف کی معلومات کی حفاظت کے لیے کمپنیوں کی ذمہ داریوں کی وضاحت کر سکیں۔
- ڈیٹا کی اخلاقیات کے اصولوں کی بشمول شفافیت، رازداری کا احترام اور جوابدہی وضاحت کر سکیں۔
- ڈیٹا اکٹھا کرنے، ذخیرہ کرنے اور شیئر کرنے کے لیے اخلاقی رہنما خطوط بشمول باخبر رضامندی اور ڈیٹا کی حفاظت کی اہمیت بیان کر سکیں۔
- ڈیٹا کی خراب حفاظت کے اثرات اور قانونی اور اخلاقی رہنما خطوط پر عمل کرنے کی اہمیت کو سمجھنے کے لیے ڈیٹا کی خلاف ورزیوں کے حقیقی زندگی کے کیس اسٹڈیز کا تجزیہ کر سکیں۔
- ڈیجیٹل مواد اور ایجادات کے تحفظ میں کاپی رائٹ، ٹریڈ مارکس اور پیٹنٹ کی اہمیت کی وضاحت اور وضاحت کر سکیں۔
- انٹلکچوئل پراپرٹی کے حقوق سے متعلق اخلاقی اور قانونی ذمہ داریوں اور ان حقوق کی خلاف ورزی کے نتائج پر تبادلہ خیال کر سکیں۔
- محفوظ آن لائن تحقیق کے لیے تکنیکوں کا استعمال کر سکیں، بشمول قابل اعتماد ذرائع کا استعمال، تصنیف کی جانچ پڑتال، اور معلومات کی کراس چیکنگ
- تحقیق کے دوران رازداری کے تحفظ کے لیے حکمت عملیوں جیسے پرائیویٹ براؤزنگ کا استعمال اور مشکوک لنکس سے بچنے کی وضاحت کر سکیں۔
- انٹرنیٹ کی لت کی علامات کو پہچانیں اور انٹرنیٹ کے متوازن استعمال کو فروغ دینے اور آف لائن سرگرمیوں میں مشغول ہونے کے لیے حکمت عملی تجویز کر سکیں۔

stepacademyofficial.com

انشائی طرز سوالات

محکمہ تعلیم کی نئی امتحانی تکنیکس (Knowledge, Understanding, Application, Analytical & Conceptual) کی روشنی میں مرتب کیے گئے انشائی طرز سوالات

11.1 کمپیوٹر کا ذمہ دارانہ استعمال

11.2 کمپیوٹر کے ذمہ دارانہ استعمال کا جائزہ

سوال 1: آج کی ڈیجیٹل دنیا میں ذمہ دار کمپیوٹر کے استعمال کی اہمیت پر تبادلہ خیال کریں۔ وضاحت کریں کہ کس طرح صحیح ہارڈ ویئر اور سافٹ ویئر کا انتخاب کمپیوٹر کے استعمال میں حفاظت، کارکردگی اور مطابقت کو متاثر کر سکتا ہے۔

جواب: کمپیوٹر کا محفوظ اور دانشمندانہ استعمال:

کمپیوٹر آج کل ہماری زندگی کا ایک لازمی حصہ چکے ہیں چاہے ہم انہیں اسکول کے کام کے لیے استعمال کر رہے ہوں، دوستوں کے ساتھ بات چیت کر رہے ہوں یا گیم کھیل رہے ہوں، کمپیوٹر کو محفوظ طریقے سے اور ذمہ داری کے ساتھ استعمال کرنا ضروری ہے۔ محفوظ اور ذمہ دار کمپیوٹر کے استعمال کا مطلب یہ جاننا ہے کہ اپنی ذاتی معلومات کی حفاظت کیسے کی جائے، ہم جو ہارڈ ویئر اور سافٹ ویئر استعمال کرتے ہیں اس کے بارے میں دانشمندانہ انتخاب کریں، اور اس بات کو یقینی بنائیں کہ ہمارا آن لائن طرز عمل قابل احترام اور اخلاقی ہے۔ ہم کمپیوٹر کو دانشمندی اور محفوظ طریقے سے استعمال کرنے کے کلیدی پہلوؤں کو تلاش کریں گے تاکہ ہم ممکنہ خطرات سے گریز کرتے ہوئے ٹیکنالوجی کے فوائد سے لطف اندوز ہو سکیں۔

کمپیوٹر کے ذمہ دارانہ استعمال کا جائزہ: ٹیکنالوجی کے ساتھ ذمہ دار ہونے کا مطلب ہے کمپیوٹر کا استعمال کرتے وقت سوچ سمجھ کر فیصلے کرنا۔ اس میں صحیح ہارڈ ویئر اور سافٹ ویئر کا انتخاب، ہمارے ڈیٹا کی حفاظت، اور انٹرنیٹ کو اس طرح استعمال کرنا شامل ہے جس سے دوسروں کا احترام ہو۔ آیئے اس پر گہری نظر ڈالیں کہ ٹیکنالوجی کو ذمہ داری کے ساتھ استعمال کرنا کیوں ضروری ہے۔ جب ہم کمپیوٹر کے بارے میں بات کرتے ہیں تو، ہارڈ ویئر مانیٹر، کی بورڈ، اور سی پی یو جیسے فزیکل حصے ہوتے ہیں، جبکہ سافٹ ویئر میں وہ پروگرام اور ایپلی کیشنز شامل ہیں جو ہم استعمال کرتے ہیں، جیسے ورڈ پروسیسرز یا گیمز۔ صحیح ہارڈ ویئر اور سافٹ ویئر کا انتخاب اہم ہے کیونکہ یہ کمپیوٹر کے استعمال کے حفاظت، کارکردگی اور مجموعی تجربے کو متاثر کر سکتا ہے۔

حفاظت: جس طرح آپ ٹوٹا ہوا یا غیر محفوظ ٹول استعمال نہیں کریں گے، اسی طرح فرسودہ یا غیر محفوظ ہارڈ ویئر یا سافٹ ویئر کا استعمال آپ کو خطرے میں ڈال سکتا ہے۔ مثال کے طور پر، تازہ ترین اینٹی وائرس سافٹ ویئر کے بغیر کمپیوٹر کا استعمال وائرس یا ہیکرز کے لیے آپ کی معلومات چوری کرنا آسان بنا سکتا ہے۔

کارکردگی: صحیح ہارڈ ویئر اور سافٹ ویئر آپ کو کاموں کو جلدی اور آسانی سے مکمل کرنے میں مدد کرتے ہیں۔ کسی پرانے کمپیوٹر پر نیا ویڈیو گیم کھیلنے کی کوشش کا تصور کریں، یہ گیم سست ہو سکتا ہے یا بالکل کام نہیں کر سکتا، جس سے اسے استعمال کرنا مایوس کن ہو جاتا ہے۔

مطابقت: اس کا مطلب یہ ہے کہ ہارڈ ویئر اور سافٹ ویئر کو ایک ساتھ اچھی طرح سے کام کرنا چاہئے۔ آپ کو ہمیشہ سافٹ ویئر پیکجوں پر سسٹم کی ضروریات کو چیک کرنا چاہیے اور مطابقت کو یقینی بنانے کے لیے انہیں اپنے کمپیوٹر کی خصوصیات سے ملانا چاہیے۔

11.3 ڈیجیٹل پلیٹ فارمز کا محفوظ اور محفوظ آپریشن

سوال 2: مختلف ڈیجیٹل پلیٹ فارمز کے محفوظ اور محفوظ آپریشن کی وضاحت کریں۔

جواب: ڈیجیٹل پلیٹ فارمز کا محفوظ اور محفوظ آپریشن:

آج کی ڈیجیٹل دنیا میں ہم مواصلات، سیکھنے، تفریح اور کام کے لیے مختلف آن لائن پلیٹ فارم اور آلات استعمال کرتے ہیں۔ اگرچہ یہ ڈیجیٹل ٹولز بہت سے فوائد پیش کرتے ہیں، لیکن ہماری ذاتی معلومات کی حفاظت اور مثبت آن لائن ماحول کو برقرار رکھنے کے لیے انہیں محفوظ اور محفوظ طریقے سے چلانا ضروری ہے۔

stepacademyofficial.com

ڈیجیٹل پلیٹ فارمز اور آلات کا محفوظ آپریشن: جب ہم ڈیجیٹل پلیٹ فارمز اور آلات کے 'محفوظ آپریشن' کے بارے میں بات کرتے ہیں، تو ہمارا مطلب ہے کہ ان کا استعمال اس طرح سے کرنا کہ جو آپ کو نقصان سے بچائے اور کسی بھی ناپسندیدہ مسائل سے بچائے۔ غور کرنے کے لیے کچھ اہم نکات یہ ہیں:

1- **مضبوط پاس ورڈز کا استعمال:** ہمیشہ اپنے اکاؤنٹس کے لیے مضبوط، منفرد پاس ورڈز بنائیں۔ ایک مضبوط پاس ورڈ میں عام طور پر حروف، اعداد اور خصوصی حروف کا مرکب شامل ہوتا ہے۔ مثال کے طور پر، "Pasword 123" استعمال کرنے کے بجائے، آپ "B3tterP@ssw0rd!" جیسی کوئی چیز استعمال کر سکتے ہیں۔

2- **باقاعدہ سافٹ ویئر اپ ڈیٹس:** اپنے آلات اور ایپلی کیشنز کو اپ ٹو ڈیٹ رکھنا حفاظت کے لیے اہم ہے۔ سافٹ ویئر اپ ڈیٹس میں اکثر اہم حفاظتی اصلاحات شامل ہوتی ہیں جو آپ کے آلے کو نئے خطرات سے بچاتی ہیں۔

3- **لنکس اور ڈاؤن لوڈ کے بارے میں محتاط رہنا:** نامعلوم لنکس پر کلک کرنے یا غیر معتبر ذرائع سے فائلیں ڈاؤن لوڈ کرنے سے گریز کریں۔ ان میں نقصان دہ سافٹ ویئر ہو سکتا ہے، جسے میلویئر کہا جاتا ہے، جو آپ کے موبائل اور کمپیوٹر کو نقصان پہنچا سکتا ہے یا آپ کی ذاتی معلومات چوری کر سکتا ہے۔

4- **رازداری کی ترتیبات کو سمجھنا:** زیادہ تر ڈیجیٹل پلیٹ فارم آپ کو یہ کنٹرول کرنے کی اجازت دیتے ہیں کہ کون آپ کی معلومات دیکھ سکتا ہے اور آن لائن آپ کے ساتھ بات چیت کر سکتا ہے۔ اپنی ذاتی معلومات کی حفاظت کے لیے اپنی رازداری کی ترتیبات کو چیک اور ایڈجسٹ کرنا ضروری ہے۔

5- **اوور شیئرنگ سے گریز کرنا:** اگرچہ آن لائن دوستوں کے ساتھ تصاویر اور اپ ڈیٹس شیئر کرنا مزہ آ سکتا ہے، لیکن آپ جو معلومات شیئر کرتے ہیں اس کا خیال رکھنا ضروری ہے۔ اپنے گھر کا پتہ، فون نمبر، یا اسکول کا نام جیسی ذاتی تفصیلات پوسٹ کرنے سے گریز کریں۔

ڈیجیٹل پلیٹ فارم کا محفوظ استعمال

ڈیجیٹل پلیٹ فارم کو محفوظ طریقے سے استعمال کرنے کا مطلب ہے اپنی معلومات کی حفاظت کے لیے اضافی اقدامات کرنا اور اس بات کو یقینی بنانا کہ آپ کی آن لائن سرگرمیاں آپ کو یا دوسروں کو خطرے میں نہ ڈالیں۔ یہاں کچھ تجاویز ہیں:

1- **ٹو فیکٹر اتھنٹی فکیشن (2FA):** ٹو فیکٹر توثیق آپ کے اکاؤنٹس میں سیکیورٹی کی ایک اضافی پرت کا اضافہ کرتی ہے۔ اپنا پاس ورڈ درج کرنے کے بعد، آپ سے معلومات کا ایک اور ٹکڑا فراہم کرنے کو کہا جائے گا، جیسے آپ کے فون پر بھیجا گیا کوڈ۔ اس سے کسی کے لیے آپ کے اکاؤنٹ کو ہیک کرنا بہت مشکل ہو جاتا ہے۔

2- **حساس لین دین کے لیے پبلک وائی فائی سے گریز کرنا:** پبلک وائی فائی نیٹ ورک، جیسے کیفے یا لائبریریوں میں، اکثر کم محفوظ ہوتے ہیں۔ ان نیٹ ورکس سے جڑے ہوئے حساس معلومات، جیسے آن لائن بینکنگ تک رسائی سے گریز کرنا بہتر ہے۔ اس کے بجائے، اس وقت تک انتظار کریں جب تک کہ آپ گھر پر کسی محفوظ، نجی نیٹ ورک پر نہ ہوں۔

3- **سکیمز سے آگاہ ہونا:** آن لائن سکیمز آپ کو دھوکہ دے کر آپ کی ذاتی معلومات دینے کے لیے بنائے جاتے ہیں۔ ان میں فشنگ ای میلز شامل ہو سکتی ہیں جو آپ کے لاگ ان کی تفصیلات مانگنے والی جائز کمپنیوں کی ہونے کا بہانہ کرتی ہیں۔ ذاتی معلومات کے لیے غیر مطلوبہ درخواستوں کے بارے میں ہمیشہ شکوک و شبہات کا اظہار کریں، اور جواب دینے سے پہلے ماخذ کی تصدیق کریں۔

4- **اپنے اکاؤنٹ کی سرگرمی کا باقاعدگی سے جائزہ لینا:** کسی بھی غیر معمولی سرگرمی کے لیے وقتاً فوقتاً اپنے آن لائن اکاؤنٹس کو چیک کریں۔ اس میں آپ کے خالیہ لاگ ان، پیغامات اور لین دین کو دیکھنا شامل ہے۔ اگر آپ کو کوئی مشکوک چیز نظر آتی ہے، جیسے کہ نامعلوم مقامات سے لاگ ان، تو فوری طور پر اپنا پاس ورڈ تبدیل کریں اور پلیٹ فارم پر سرگرمی کی اطلاع دیں۔

5- **اہم ڈیٹا کا بیک اپ لینا:** اپنے ڈیٹا کا باقاعدگی سے بیک اپ لینا اس بات کو یقینی بناتا ہے کہ اگر آپ کے آلے میں کچھ غلط ہو جائے تو آپ

stepacademyofficial.com

اہم معلومات سے محروم نہیں ہوں گے۔ آپ اپنے ڈیٹا کا بیک اپ بیرونی ہارڈ ڈرائیو یا کلاؤڈ اسٹوریج سروس جیسے گوگل ڈرائیو یا ڈراپ باکس میں لے سکتے ہیں۔

سوال 3: آن لائن برتاؤ میں بہترین طرزِ عمل کیا ہیں؟

جواب: سوشل میڈیا، ای میل، کلاؤڈ سروسز اور آن لائن ایپلی کیشنز کا ذمہ دارانہ استعمال:

آج کی ڈیجیٹل دنیا میں ہم ہر روز سوشل میڈیا، ای میل، کلاؤڈ سروسز اور آن لائن ایپلی کیشنز کا استعمال کرتے ہیں۔ اگرچہ یہ آلات ہماری زندگیوں کو آسان اور زیادہ مربوط بناتے ہیں، لیکن ان کا ذمہ داری سے استعمال کرنا ضروری ہے۔ سوشل میڈیا، ای میل، کلاؤڈ سروسز اور آن لائن ایپلی کیشنز جیسے ڈیجیٹل پلیٹ فارمز کا استعمال ہماری روزمرہ کی زندگی کا حصہ بن چکا ہے۔ تاہم، اپنی حفاظت اور دوسروں کی حفاظت کو یقینی بنانے کے لیے ان ٹولز کو ذمہ داری کے ساتھ استعمال کرنا ضروری ہے۔

سوشل میڈیا: فیس بک، انسٹاگرام اور ایکس (سابقہ ٹویٹر) جیسے سوشل میڈیا پلیٹ فارم ہمیں دوستوں سے جڑنے اور معلومات کا اشتراک کرنے کی اجازت دیتے ہیں۔ لیکن پوسٹ کرنے سے پہلے سوچنا ضروری ہے۔ ہمیشہ ذاتی معلومات، جیسے اپنے گھر کا پتہ یا فون نمبر، عوامی طور پر شیئر کرنے سے گریز کریں۔

ای میل: ای میل مواصلات کے لیے ایک مفید ذریعہ ہے، خاص طور پر اسکول اور کام کے لیے۔ تاہم، نامعلوم بھیجنے والوں کی ای میلز کھولتے وقت محتاط رہنا ضروری ہے۔ ان میں نقصان دہ لنکس یا منسلک ہو سکتے ہیں۔

کلاؤڈ سروسز: کلاؤڈ سروسز جیسے گوگل ڈرائیو یا ڈراپ باکس آپ کو فائلوں کو آن لائن اسٹور اور شیئر کرنے کی اجازت دیتی ہیں۔ اگرچہ یہ خدمات آسان ہیں، لیکن ان کا دانشمندی سے استعمال کرنا ضروری ہے۔ اپنے اکاؤنٹس کی حفاظت کے لیے ہمیشہ مضبوط پاس ورڈ استعمال کریں اور کلاؤڈ اسٹوریج کے ذریعے حساس معلومات، جیسے پاس ورڈ یا مالی تفصیلات شیئر کرنے سے گریز کریں۔

آن لائن ایپلی کیشنز: آن لائن ایپلی کیشنز، جیسے گیم، لرننگ ایپس، یا شاپنگ پلیٹ فارم، تفریحی اور مفید ہیں لیکن خطرات بھی پیدا کر سکتے ہیں۔ نقصان دہ سافٹ ویئر ڈاؤن لوڈ کرنے سے بچنے کے لیے صرف گوگل پلے اسٹور یا ایپل ایپ اسٹور جیسے قابل اعتماد ذرائع سے ایپس ڈاؤن لوڈ کرنا یقینی بنائیں۔

رازداری کی ترتیبات اور ڈیٹا کی حفاظت کے اقدامات کی اہمیت:

رازداری کی ترتیبات اور ڈیٹا کی حفاظت کے اقدامات ضروری ٹولز ہیں جو ڈیجیٹل پلیٹ فارمز کا استعمال کرتے ہوئے آپ کی ذاتی معلومات کی حفاظت میں مدد کرتے ہیں۔

رازداری کی ترتیبات: زیادہ تر آن لائن پلیٹ فارم، بشمول سوشل میڈیا اور ای میل خدمات، آپ کو رازداری کی ترتیبات کو ایڈجسٹ کرنے کی اجازت دیتے ہیں تاکہ یہ کنٹرول کیا جا سکے کہ آپ کی معلومات کون دیکھ سکتا ہے۔ مثال کے طور پر، فیس بک پر، آپ انتخاب کر سکتے ہیں کہ آپ کی پوسٹوں کو کون دیکھ سکتا ہے۔ عوام، دوست، یا صرف آپ۔ آپ کی ذاتی معلومات کی حفاظت کو یقینی بنانے کے لیے اپنی رازداری کی ترتیبات کا باقاعدگی سے جائزہ لینا اور اپ ڈیٹ کرنا ضروری ہے۔

ڈیٹا کی حفاظت کے اقدامات: ڈیٹا کی حفاظت کے اقدامات آپ کی معلومات کو غیر مجاز رسائی سے بچانے میں مدد کرتے ہیں۔ آپ کے ہر آن لائن اکاؤنٹ کے لیے مضبوط، منفرد پاس ورڈ کا استعمال آپ کے ڈیٹا کو محفوظ رکھنے کے آسان ترین اور موثر ترین طریقوں میں سے ایک ہے۔ مثال کے طور پر، ''Password123'' استعمال کرنے کے بجائے، ایک ایسا پاس ورڈ بنائیں جو حروف، اعداد اور علامتوں کو یکجا کرے، جیسے 'S3cur3!Passw0rd' پاس ورڈ۔

11.4 قانونی اور اخلاقی فریم ورک

سوال 4: ہماری ذاتی معلومات کو کس طرح ہینڈل کیا جاتا ہے؟ اخلاقی فریم ورک کے ساتھ اس کی وضاحت کریں۔

جواب: رازداری کے لیے قانونی فریم ورک:

رازداری کے قوانین اور ان کے اثرات کو سمجھنا: یہ قوانین اس بات کو یقینی بناتے ہیں کہ کمپنیاں اور تنظیمیں ہمارے ڈیٹا کو ذمہ داری کے ساتھ سنبھالتی

stepacademyofficial.com

ہیں۔ جب ہم انٹرنیٹ استعمال کرتے ہیں، تو ہم اکثر ذاتی تفصیلات جیسے اپنے نام، پتے، یا یہاں تک کہ جو ہم خریدنا پسند کرتے ہیں ان کا اشتراک کرتے ہیں۔ رازداری کے قوانین اس بات کو یقینی بنانے میں مدد کرتے ہیں کہ اس معلومات کو محفوظ رکھا جائے اور اس کا غلط استعمال نہ ہو۔ ان قوانین کو سمجھنا ضروری ہے کیونکہ وہ آپ کو اپنی ذاتی معلومات کو کنٹرول کرنے کا اختیار دیتے ہیں۔ اگر کوئی کمپنی آپ کے ڈیٹا کا غلط استعمال کرتی ہے۔ جیسے کہ آپ کی اجازت کے بغیر اسے شیئر کرنے سے، آپ کو قانونی کارروائی کرنے کا حق حاصل ہے۔

صارف کی رازداری اور غیر مجاز رسائی کے نتائج کے تحفظ کے قوانین: آن لائن آپ کی رازداری کے تحفظ کے لیے مخصوص قوانین بنائے گئے ہیں۔ یہ قوانین کسی کے لیے اجازت کے بغیر آپ کی ذاتی معلومات تک رسائی کو غیر قانونی بناتے ہیں۔ مثال کے طور پر، اگر کوئی آپ کے ای میل یا سوشل میڈیا اکاؤنٹ کو ہیک کرتا ہے، تو وہ قانون کی خلاف ورزی کر رہا ہے۔ آپ کی معلومات تک غیر مجاز رسائی سنگین مسائل کا باعث بن سکتی ہے، جیسے شناخت کی چوری یا دھوکہ دہی۔ اس کی روک تھام کے لیے، رازداری کے قوانین کمپنیوں کو آپ کے ڈیٹا کی حفاظت کے لیے خفیہ کاری جیسے مضبوط حفاظتی اقدامات کو نافذ کرنے کی ضرورت ہوتی ہے۔ اگر کوئی کمپنی آپ کی معلومات کی حفاظت کرنے میں ناکام رہتی ہے تو انہیں ذمہ دار ٹھہرایا جا سکتا ہے اور انہیں قانونی سزاؤں کا سامنا کرنا پڑ سکتا ہے۔

ڈیٹا اخلاقیات اور ذمہ دارانہ استعمال:

ڈیٹا کی اخلاقیات اور ڈیٹا ہینڈلنگ کو کنٹرول کرنے والے اصول:

ڈیٹا اخلاقیات صحیح کام کرنے کے بارے میں ہے جب یہ جمع کرنے، ذخیرہ کرنے اور معلومات کا استعمال کریں۔ صرف اس وجہ سے کہ ہم بہت زیادہ ڈیٹا اکٹھا کر سکتے ہیں اس کا مطلب یہ نہیں ہے کہ ہمیں اسے اپنی مرضی کے مطابق استعمال کرنا چاہیے۔ ڈیٹا کی اخلاقیات معلومات کو منصفانہ اور ذمہ داری کے ساتھ استعمال کرنے میں ہماری رہنمائی کرتی ہے۔ ڈیٹا اخلاقیات کے اصولوں میں شفافیت، رازداری کا احترام اور جواب دہی شامل ہیں۔ اس کا مطلب یہ ہے کہ ڈیٹا کو کس طرح استعمال کیا جاتا ہے، لوگوں کی ذاتی معلومات کی حفاظت کرنا، اور کچھ غلط ہونے کی صورت میں ذمہ داری لینا۔

ڈیٹا اکٹھا کرنے، ذخیرہ کرنے اور شیئر کرنے میں اخلاقی تحفظات:

جب ڈیٹا اکٹھا کیا جاتا ہے، ذخیرہ کیا جاتا ہے، یا شیئر کیا جاتا ہے، تو ذہن میں رکھنے کے لیے اہم اخلاقی تحفظات ہوتے ہیں۔ ڈیٹا اکٹھا کرنا ہمیشہ اس شخص کی رضامندی سے کیا جانا چاہیے۔ اس کا مطلب یہ ہے کہ معلومات اکٹھا کرنے سے پہلے اس شخص کو اس سے اتفاق کرنا چاہیے۔

- ڈیٹا کو ذخیرہ کرنے کے لیے بھی ذمہ داری کی ضرورت ہوتی ہے۔ ڈیٹا کو محفوظ رکھا جانا چاہیے تاکہ غیر مجاز افراد اس تک رسائی حاصل نہ کر سکیں۔ مثال کے طور پر، طبی ریکارڈ کو محفوظ کرنے کے لیے مضبوط تحفظ کی ضرورت ہوتی ہے کیونکہ یہ معلومات نجی اور حساس ہوتی ہے۔
- ڈیٹا کا اشتراک احتیاط سے اور صرف ضرورت پڑنے پر ہی کیا جانا چاہیے۔ مثال کے طور پر، کوئی اسکول آپ کے گریڈ آپ کے والدین کے ساتھ شیئر کر سکتا ہے، لیکن اسے آپ کی اجازت کے بغیر دوسرے طلبا کے ساتھ اس کو شیئر نہیں چاہیے۔ اخلاقی ہونے کا مطلب یہ سوچنا ہے کہ معلومات کا اشتراک دوسروں کو کس طرح متاثر کر سکتا ہے اور اس طرح کام کرنا جس سے ان کے حقوق کا احترام ہو۔

ڈیٹا کے استعمال اور انتظام کے لیے اخلاقی رہنما خطوط

ڈیٹا کے استعمال کے لیے اخلاقی رہنما خطوط میں اس بات کو یقینی بنانا شامل ہے کہ ڈیٹا کو اس مقصد کے لیے استعمال کیا جائے جس کا یہ ارادہ کیا گیا تھا اور یہ اس شخص کو فائدہ پہنچاتا ہے جس نے اسے فراہم کیا تھا۔ ڈیٹا کا غلط استعمال۔ جیسے کہ اسے بغیر رضامندی کے تیسرے فریق کو بیچنا غیر اخلاقی ہے اور اعتماد کے نقصان کا باعث بن سکتا ہے۔ ان ہدایات میں شامل ہیں:

- **باخبر رضامندی:** کسی کا ڈیٹا اکٹھا کرنے سے پہلے ہمیشہ اجازت طلب کریں۔ مثال کے طور پر، کسی ویب سائٹ کو یہ پوچھنا چاہیے کہ کیا ایسا کرنے سے پہلے آپ کی سرگرمی کو ٹریک کرنا ٹھیک ہے۔
- **ڈیٹا مائنسائزیشن:** صرف مطلوبہ ڈیٹا اکٹھا کریں۔ اگر آپ سروے کر رہے ہیں تو غیر ضروری ذاتی تفصیلات نہ پوچھیں۔
- **ڈیٹا سیکیورٹی:** اپنے جمع کردہ ڈیٹا کی حفاظت کریں۔ معلومات کو محفوظ رکھنے کے لیے مضبوط پاس ورڈ اور خفیہ کاری کا استعمال کریں۔

stepacademyofficial.com

https://stepacademyofficial.com/

- **احتساب:** اگر کچھ غلط ہو جائے تو ذمہ داری قبول کریں۔ اگر ڈیٹا کی خلاف ورزی ہوئی ہے تو متاثرہ افراد کو مطلع کریں اور مسئلے کو حل کرنے کے لیے اقدامات کریں۔

11.5 دانشورانہ املاک کے تصورات

سوال 5: دانشورانہ املاک کے حقوق کی مختلف اقسام پر تبادلہ خیال کریں، بشمول کاپی رائٹ، ٹریڈ مارک، اور پیٹنٹ۔

جواب: دانشورانہ املاک کے حقوق اہم ہیں کیونکہ وہ افراد اور تنظیموں کی تخلیقات اور نظریات کی حفاظت کرتے ہیں۔ جب کوئی کوئی نئی چیز تخلیق کرتا ہے، جیسے موسیقی کا ٹکڑا، کتاب، یا ایجاد، تو اسے یہ اختیار حاصل ہوتا ہے کہ اسے کس طرح استعمال کیا جائے۔

کاپی رائٹ، ٹریڈ مارک، پیٹنٹ، اور ڈیجیٹل مواد میں ان کی اہمیت:

(i) کاپی رائٹ ایک قانونی حق ہے جو تخلیق کاروں کو اپنے اصل کاموں، جیسے موسیقی، کتابیں، فلمیں اور سافٹ ویئر پر کنٹرول دیتا ہے۔ مثال کے طور پر، جب کوئی مصنف کوئی کتاب لکھتا ہے، تو اس کے پاس یہ فیصلہ کرنے کے لیے کاپی رائٹ ہوتا ہے کہ کتاب کو کس طرح شائع کیا جاتا ہے، شیئر کیا جاتا ہے، یا موافق بنایا جاتا ہے۔ اس کا مطلب ہے کہ مصنف کی اجازت کے بغیر کوئی اور کتاب کاپی یا تقسیم نہیں کر سکتا۔

(ii) ٹریڈ مارک وہ علامتیں، نام یا نعرے ہوتے ہیں جو کمپنیاں اپنی مصنوعات یا خدمات کو دوسروں سے ممتاز کرنے کے لیے استعمال کرتی ہیں۔ مثال کے طور پر، ''Nike'' 'Swoosh' لوگو ایک ٹریڈ مارک ہے۔ ٹریڈ مارک برانڈ کی شناخت کی حفاظت کرتے ہیں، اس لیے کوئی دوسری کمپنی صارفین کو الجھانے کے لیے اسی طرح کی علامت استعمال نہیں کر سکتی۔

(iii) پیٹنٹ نئی ایجادات یا عمل کی حفاظت کرتے ہیں، جس سے موجد کو ایک مخصوص مدت کے لیے ایجاد بنانے، استعمال کرنے یا فروخت کرنے کے خصوصی حقوق ملتے ہیں۔

مثال کے طور پر، اگر کوئی نئی قسم کا اسمارٹ فون ایجاد کرتا ہے، تو وہ دوسروں کو بغیر اجازت کے اسی طرح کا فون بنانے یا فروخت کرنے سے روکنے کے لیے اسے پیٹنٹ کرا سکتا ہے۔

دانشورانہ املاک کے حقوق سے متعلق اخلاقی اور قانونی ذمہ داریاں:

دانشورانہ املاک کے حقوق کا احترام کرنے کا مطلب یہ سمجھنا ہے کہ اجازت کے بغیر کسی اور کے کام کی نقل، اشتراک یا استعمال کرنا نہ صرف غیر اخلاقی ہے بلکہ غیر قانونی بھی ہے۔ مثال کے طور پر، فلموں یا سافٹ ویئر کو ان کے لیے ادائیگی کیے بغیر ڈاؤن لوڈ کرنا کاپی رائٹ قانون کی خلاف ورزی ہے۔ تخلیق کاروں کی حمایت کرنے اور ان کے حقوق کا احترام کرنے کے لیے ہمیشہ اجازت لینا یا قانونی طور پر مواد خریدنا ضروری ہے۔

کمپیوٹنگ میں قانونی تعمیل: سافٹ ویئر پائریسی سافٹ ویئر کی غیر قانونی کاپی، تقسیم یا استعمال ہے۔ جب آپ سافٹ ویئر خریدتے ہیں، تو آپ اصل میں اسے استعمال کرنے کا لائسنس خرید رہے ہوتے ہیں، نہ کہ خود سافٹ ویئر۔ مناسب لائسنس کے بغیر اس کی نقل کرنا اور اسے دوسروں کے ساتھ شیئر کرنا قانون کے خلاف ہے۔ پائریسی نقصان دہ ہے کیونکہ یہ سافٹ ویئر ڈویلپرز کو اس رقم سے دھوکہ دیتا ہے جس کی انہیں اپنی مصنوعات بنانے اور بہتر بنانے کے لیے ضرورت ہوتی ہے۔ دانشورانہ املاک کے حقوق کو سمجھنے اور ان کا احترام کرنے سے، ہم سب ایک منصفانہ اور قانونی ڈیجیٹل ماحول میں حصہ ڈال سکتے ہیں۔

11.6 ذمہ دار انٹرنیٹ استعمال

سوال 6: محفوظ اور قابل اعتماد آن لائن تحقیق کے انعقاد کے لیے موثر تکنیکوں کا خاکہ کریں۔

جواب: ڈیٹا کی محفوظ تلاش اور آن لائن تحقیق:

محفوظ ڈیٹا کی تلاش اور اعتبار کی تشخیص کے لیے تکنیکیں: آن لائن معلومات کی تلاش کرتے وقت، یہ ضروری ہے کہ اسے محفوظ طریقے سے کیا جائے اور اس بات کو یقینی بنایا جائے کہ جو معلومات آپ کو ملتی ہیں وہ قابل بھروسہ اور قابل اعتماد ہے۔ یہاں کچھ تجاویز ہیں:

stepacademyofficial.com

قابل اعتماد ذرائع کا استعمال کریں: ہمیشہ معروف ویب سائٹس استعمال کرنے کی کوشش کریں، جیسے تعلیمی ادارے (.edu)، سرکاری سائٹس (.gov)، اور معروف تنظیمیں (.org)۔ مثال کے طور پر اگر آپ موسمیاتی تبدیلی پر تحقیق کر رہے ہیں، تو نیشنل جیوگرافک یا سرکاری ایجنسیوں جیسی ویب سائٹیں قابل اعتماد ذرائع ہوں گی۔

مصنف کو چیک کریں: مواد کے مصنف کے بارے میں معلومات تلاش کریں۔ کیا وہ اس شعبے میں ماہر ہیں؟ کیا ان کے پاس اپنے دعوؤں کی پشت پناہی کرنے کے لیے اسناد ہیں؟ مثال کے طور پر طبی مشورے پر ایک مضمون کسی مستند ڈاکٹر یا ہیلتھ کیئر پروفیشنل کے ذریعے لکھا جانا چاہیے۔

- **کراس چیک کی معلومات:** معلومات کی درستگی کی تصدیق کرنے کے لیے مختلف ذرائع کو چیک۔ اگر کئی قابل اعتماد ویب سائٹیں ایک ہی حقائق پر متفق ہیں، تو معلومات کے درست ہونے کا امکان زیادہ ہے۔
- **سنسنی خیز سرخیوں پر شک کریں:** ایسی ویب سائٹس سے گریز کریں جو آپ کی توجہ حاصل کرنے کے لیے بنائی گئی سنسنی خیز یا گمراہ کن سرخیاں استعمال کرتی ہیں۔ یہ سائٹیں اکثر غلط معلومات یا 'جعلی خبریں' پھیلاتی ہیں۔ مثال کے طور پر، ایک سرخی جو کسی بیماری کے معجزانہ علاج کا دعویٰ کرتی ہے، ممکنہ طور پر قابل اعتبار نہیں ہے۔

آن لائن تحقیق اور معلومات جمع کرنے کے دوران رازداری کے خطرات سے بچنا:

آن لائن تحقیق کرتے وقت، اپنی رازداری کی حفاظت کرنا ضروری ہے۔ یہاں طریقہ ہے:

- **پرائیویٹ براؤزنگ کا استعمال کریں:** زیادہ تر ویب براؤزر ایک نجی یا ان کوگنیٹو موڈ پیش کرتے ہیں جو آپ کی براؤزنگ ہسٹری یا ذاتی معلومات کو محفوظ نہیں کرتا ہے۔ حساس موضوعات پر تحقیق کرتے وقت یہ مفید ہے۔
- **ذاتی معلومات سے محتاط رہیں:** غیر واقف ویب سائٹس پر ذاتی معلومات درج کرنے سے گریز کریں۔ مثال کے طور پر، اگر کوئی ویب سائٹ معلومات تک رسائی کے لیے آپ کا ای میل ایڈریس یا فون نمبر مانگتی ہے، تو غور کریں کہ آیا یہ خطرے کے قابل ہے یا نہیں۔
- **مشکوک لنکس سے بچیں:** اگر آپ کو ایسے لنکس ملتے ہیں جو عجیب لگتے ہیں یا بہت اچھے لگتے ہیں تو ان پر کلک نہ کریں۔ وہ نقصان دہ ویب سائٹس کا باعث بن سکتی ہیں جو آپ کی ذاتی معلومات چوری کرنے کی کوشش کرتی ہیں۔

سوال 7: انٹرنیٹ کی عادت کے تصور اور افراد پر اس کے ممکنہ اثرات پر بحث کریں۔ نشے کی علامات کو پہچاننا، وقت کی حدود طے کرنا اور آف لائن سرگرمیوں کو تلاش کرنا انٹرنیٹ کے متوازن استعمال کو فروغ دینے میں کس طرح مدد کر سکتا ہے؟

جواب: انٹرنیٹ کی عادت سے بچاؤ:

انٹرنیٹ کی عادت کو سمجھنا اور متوازن استعمال کو فروغ دینا: انٹرنیٹ کی عادت اس وقت ہوتی ہے جب کوئی شخص آن لائن اتنا وقت گزارتا ہے کہ یہ ان کی روزمرہ کی زندگی میں مداخلت کرنے لگتا ہے۔ انٹرنیٹ کی عادت کی علامات کو پہچاننا اور اس کی روک تھام کے لیے اقدامات کرنا ضروری ہے۔

- **علامات کو پہچاننا:** اگر آپ کو انٹرنیٹ کا استعمال بند کرنا مشکل لگتا ہے، یہاں تک کہ جب سونے، پڑھنے، یا خاندان اور دوستوں کے ساتھ وقت گزارنے کا وقت ہو، تو آپ کو ایک غیر صحت بخش عادت پڑ سکتی ہے۔ مثال کے طور پر، اگر آپ ہر روز گھنٹوں سوشل میڈیا کے ذریعے اسکرولنگ کرتے ہیں اور اپنے ہوم ورک کو نظر انداز کرتے ہیں، تو یہ انٹرنیٹ کی عادت کی علامت ہو سکتی ہے۔
- **وقت کی حدود طے کریں:** انٹرنیٹ کی عادت کو روکنے کا ایک طریقہ یہ ہے کہ اپنے انٹرنیٹ کے استعمال پر وقت کی حدود طے کریں۔ مثال کے طور پر، آپ ہر روز سوشل میڈیا پر ایک گھنٹے سے زیادہ نہ گزارنے کا فیصلہ کر سکتے ہیں اور اس پر قائم رہ سکتے ہیں۔
- **آف لائن سرگرمیاں تلاش کریں:** اپنے آن لائن وقت کو آف لائن سرگرمیوں جیسے کھیلوں، پڑھنے، یا ذاتی طور پر دوستوں کے ساتھ وقت گزارنے کے ساتھ متوازن کریں۔ اس سے آپ کو صحت مند طرز زندگی برقرار رکھنے میں مدد ملتی ہے۔

stepacademyofficial.com

ڈیجیٹل فلاح و بہبود اور صحت مند آن لائن عادات کو فروغ دینے کی حکمت عملی:

ڈیجیٹل فلاح و بہبود کو برقرار رکھنے کا مطلب انٹرنیٹ کو صحت مند اور متوازن طریقے سے استعمال کرنا ہے۔ یہاں کچھ حکمت عملی ہیں:

- **باقاعدگی سے وقفے لیں:** طویل عرصے تک انٹرنیٹ استعمال کرتے وقت، اپنی آنکھوں کو آرام دینے اور اپنے دماغ کو صاف کرنے کے لیے وقفے لیں۔ مثال کے طور پر، اگر آپ آن لائن تعلیم حاصل کر رہے ہیں، تو ہر گھنٹے 5 منٹ کا وقفہ لے کر آرام کریں۔
- **ٹیکنالوجی کو دانشمندی سے استعمال کریں:** ایسی ایپس یا فیچرز کا استعمال کریں جو آپ کو آن لائن اپنے وقت کا انتظام کرنے میں مدد کرتی ہیں۔ کچھ ایپس آپ کے اسکرین ٹائم کو ٹریک کر سکتی ہیں اور آپ کو وقفہ لینے کے لیے ریمائنڈر بھیج سکتی ہیں۔
- **اپنی ذہنی صحت کا خیال رکھیں:** اگر آن لائن ہونے سے آپ کو تناؤ، بے چینی یا ناخوش محسوس ہوتا ہے، تو یہ وقت کم کرنے کا ہو سکتا ہے۔ مثال کے طور پر، اگر آپ مسلسل اطلاعات سے مغلوب محسوس کرتے ہیں، تو انہیں تھوڑی دیر کے لیے بند کرنے پر غور کریں۔

سوشل نیٹ ورکنگ سیفٹی اور آن لائن تعاملات:

رازداری کی ترتیبات، ذمہ دارانہ اشتراک، اور آن لائن آداب:

سوشل نیٹ ورکنگ پلیٹ فارم ہمیں دوستوں کے ساتھ جڑنے اور اپنی زندگی بانٹنے کی اجازت دیتے ہیں، لیکن ایسا محفوظ طریقے سے اور احترام کے ساتھ کرنا ضروری ہے۔

- **اپنی پرائیویسی کی ترتیبات کو ایڈجسٹ کریں:** اس بات کو یقینی بنائیں کہ آپ کے سوشل میڈیا اکاؤنٹس پرائیویٹ پر سیٹ ہیں، تاکہ صرف وہی لوگ آپ کی پوسٹس دیکھ سکیں جن پر آپ اعتماد کرتے ہیں۔ مثال کے طور پر، انسٹاگرام پر، آپ اپنا اکاؤنٹ 'پرائیویٹ' پر سیٹ کر سکتے ہیں تاکہ صرف منظور شدہ فالوورز ہی آپ کا مواد دیکھ سکیں۔
- **شیئر کرنے سے پہلے سوچیں:** کچھ بھی آن لائن پوسٹ کرنے سے پہلے ہمیشہ اچھی طرح سوچیں۔ ذاتی معلومات کا اشتراک کرنے سے گریز کریں جیسے آپ کا پتہ، فون نمبر، یا کوئی بھی ایسی تفصیلات جو آپ کو خطرے میں ڈال سکتی ہیں۔ مثال کے طور پر اگر آپ اپنے نئے گھر کی تصویر شیئر کرنا چاہتے ہیں، تو یقینی بنائیں کہ یہ آپ کے صحیح مقام کو ظاہر نہیں کرتا ہے۔
- **اچھے آن لائن آداب کی مشق کریں:** اپنی آن لائن بات چیت میں احترام کا مظاہرہ کریں۔ اس کا مطلب ہے شائستہ زبان کا استعمال کرنا، دلائل سے گریز کرنا، اور افواہوں یا غلط معلومات کو نہ پھیلانا۔ مثال کے طور پر، اگر آپ کسی کی پوسٹ سے متفق نہیں ہیں، تو ان کی توہین کیے بغیر احترام کے ساتھ اپنی رائے کا اظہار کریں۔

سائبر بلی انگ، ہراساں کرنے اور قابل احترام آن لائن تعاملات سے نمٹنا

سائبر غنڈہ گردی اور آن لائن ہراساں کرنا سنگین مسائل ہیں جو لوگوں کو جذباتی اور ذہنی طور پر تکلیف پہنچا سکتے ہیں۔ ان سے نمٹنے کا طریقہ یہ ہے:

- **سائبر دھونس کو پہچانیں:** سائبر بلی انگ میں انٹرنیٹ کا استعمال دوسروں کو نقصان پہنچانے یا ہراساں کرنے کے لیے کرنا شامل ہے۔ اس میں مضحکہ خیز پیغامات بھیجنا، افواہیں پھیلانا، یا کسی کی اجازت کے بغیر شرمناک تصاویر پوسٹ کرنا شامل ہو سکتا ہے۔
- **رپورٹ کریں اور بلاک کریں:** اگر آپ سائبر بلی انگ کا تجربہ کرتے ہیں یا دیکھتے ہیں، تو اس کی اطلاع پلیٹ فارم پر دیں اور ذمہ دار شخص کو بلاک کریں۔ زیادہ تر سوشل میڈیا پلیٹ فارمز کے پاس ایسا کرنے میں آپ کی مدد کرنے کے لیے ٹولز ہوتے ہیں۔ مثال کے طور پر، فیس بک پر، آپ کسی کو آپ سے رابطہ کرنے یا آپ کا پروفائل دیکھنے سے روکنے کے لیے بلاک کر سکتے ہیں۔
- **دوسروں کی حمایت کریں:** اگر آپ دیکھتے ہیں کہ کسی کو آن لائن غنڈہ گردی کا نشانہ بنایا جا رہا ہے تو اپنی مدد کی پیشکش کریں۔ آپ غنڈہ گردی کی اطلاع دے کر یا صرف مہربان الفاظ پیش کر کے ان کے لیے کھڑے ہو سکتے ہیں۔ اس سے ان کے احساس میں بڑا فرق پڑ سکتا ہے۔

stepacademyofficial.com

قابل احترام تعاملات کی مشق کریں: ہمیشہ دوسروں کے ساتھ آن لائن احترام کے ساتھ سلوک کریں، جیسا کہ آپ ذاتی طور پر کرتے ہیں۔ منفی تبصرے کرنے سے گریز کریں، اور اس بارے میں سوچیں کہ آپ کے الفاظ کسی اور کو کس طرح متاثر کر سکتے ہیں۔ مثال کے طور پر، اگر آپ کو کوئی پوسٹ نظر آتی ہے جو آپ کو پسند نہیں ہے، تو تکلیف دہ تبصرہ کرنے سے بہتر ہے کہ اس کے آگے اسکرال کریں۔

11.7 معاشرے پر کمپیوٹنگ کا اثر

سوال 8: ہمارے معاشرے پر کمپیوٹنگ کے اثرات کو مختصر طور پر بیان کریں۔

جواب: کمپیوٹنگ ٹیکنالوجی کا ہماری دنیا پر نمایاں اثر پڑتا ہے۔ یہ ہمارے رہنے، کام کرنے اور ایک دوسرے کے ساتھ بات چیت کرنے کے طریقے کو تبدیل کرتا ہے۔

ماحولیاتی، اخلاقی، قانونی، سماجی، اقتصادی اور ثقافتی اثرات:

کمپیوٹنگ ہماری زندگیوں کے بہت سے پہلوؤں کو متاثر کرتی ہے، ماحول سے لے کر ہمارے ثقافتی طریقوں تک۔ یہ ہے طریقہ:

ماحولیاتی اثرات: کمپیوٹنگ آلات، جیسے کمپیوٹر اور اسمارٹ فونز، کو چلانے کے لیے توانائی اور تیاری کے لیے مواد کی ضرورت ہوتی ہے۔ ان آلات کی پیداوار اور ضائع کرنا ماحول کو نقصان پہنچا سکتا ہے۔ مثال کے طور پر الیکٹرانکس میں استعمال ہونے والی دھاتوں کی کان کنی آلودگی کا سبب بن سکتی ہے۔

- **اخلاقی اثر:** کمپیوٹنگ اس بارے میں اخلاقی سوالات اٹھاتی ہے کہ ہم ٹیکنالوجی کو کس طرح استعمال کرتے ہیں۔ مثال کے طور پر، اجازت کے بغیر کسی اور کے کام کا استعمال کرنا غیر اخلاقی ہے۔ یہی وجہ ہے کہ کاپی رائٹ کے قوانین کا احترام کرنا اور اصل تخلیق کاروں کو کریڈٹ دینا ضروری ہے۔
- **قانونی اثر:** کمپیوٹنگ میں قانونی مسائل بھی شامل ہیں، جیسے رازداری کے قوانین اور انٹرنیٹ کے استعمال سے متعلق ضابطے۔ مثال کے طور پر، قوانین ہماری ذاتی معلومات کو کمپنیوں یا افراد کے غلط استعمال سے بچاتے ہیں۔ ان قوانین کو سمجھنے سے ہمیں آن لائن اپنے حقوق کے تحفظ میں مدد ملتی ہے۔
- **سماجی اثر:** ٹیکنالوجی بدلتی ہے کہ ہم ایک دوسرے کے ساتھ کس طرح بات چیت کرتے ہیں۔ سوشل میڈیا ہمیں دنیا بھر میں دوستوں اور کنبہ کے ساتھ جڑنے کی اجازت دیتا ہے، لیکن یہ سائبر دھونس جیسے مسائل کا باعث بھی بن سکتا ہے۔ ان اثرات سے آگاہ ہونے سے ہمیں ٹیکنالوجی کو مثبت طریقوں سے استعمال کرنے میں مدد ملتی ہے۔
- **اقتصادی اثر:** کمپیوٹنگ ٹیکنالوجی نے نئی صنعتیں اور روزگار کے مواقع پیدا کیے ہیں۔ مثال کے طور پر، سافٹ ویئر کی ترقی اور ڈیجیٹل مارکیٹنگ عروج کے شعبے ہیں۔ تاہم، یہ روایتی ملازمتوں کو بھی متاثر کرتا ہے، کیونکہ آٹومیشن کچھ کرداروں کی جگہ لے سکتا ہے۔ ان تبدیلیوں کو سمجھنے سے ہمیں ترقی پذیر ملازمت کے بازار کے مطابق ڈھالنے میں مدد ملتی ہے۔
- **ثقافتی اثر:** ٹیکنالوجی ہماری ثقافت پر اثر انداز ہوتی ہے کہ ہم کس طرح مواد تخلیق اور اشتراک کرتے ہیں۔ مثال کے طور پر سوشل میڈیا کے رجحانات تیزی سے پھیل سکتے ہیں فیشن، موسیقی اور دیگر ثقافتی پہلوؤں کو متاثر کرتے ہیں۔

عالمی تجارت، مواصلات اور ثقافت میں کمپیوٹنگ کا کردار:

ارتقاء کمپیوٹنگ نے تبدیل کر دیا ہے کہ ہم کس طرح تجارت کرتے ہیں، بات چیت کرتے ہیں اور ثقافت کو عالمی سطح پر بانٹتے ہیں:

- **عالمی تجارت:** کمپیوٹنگ سسٹم دنیا بھر میں مصنوعات کی خریداری اور فروخت کو آسان بناتے ہیں۔ ایمیزون، علی ایکسپریس اور دراز جیسے آن لائن شاپنگ پلیٹ فارم ہمیں مختلف ممالک سے اشیا خریدنے کی اجازت دیتے ہیں۔ کمپیوٹر کاروباروں کو انوینٹری کا انتظام کرنے، لین دین پر کارروائی کرنے اور ترسیل کو مؤثر طریقے سے ٹریک کرنے میں مدد کرتے ہیں۔
- **مواصلات:** ٹیکنالوجی ای میل، میسجنگ ایپس اور سوشل میڈیا کے ذریعے فوری مواصلات کو قابل بناتی ہے۔ مثال کے طور پر، ویڈیو کالز لوگوں

stepacademyofficial.com

کو طویل فاصلے پر دوستوں کے ساتھ کام کرنے یا چیٹ کرنے کی اجازت دیتی ہیں، جس سے عالمی تعاون اور ذاتی رابطے آسان ہو جاتے ہیں۔

- **ثقافتی ارتقاء:** کمپیوٹنگ ثقافتوں کو بانٹنے اور پھیلانے میں مدد کرتی ہے۔ یوٹیوب اور انسٹاگرام جیسے آن لائن پلیٹ فارم مختلف ثقافتوں کے لوگوں کو اپنی روایات اور نظریات کا اشتراک کرنے دیتے ہیں۔

کمپیوٹنگ کی ترقی کے فوائد اور خطرات (سوشل نیٹ ورکنگ، غلط معلومات)

کمپیوٹنگ کی ترقی سے بہت سے فوائد ہوتے ہیں لیکن کچھ خطرات بھی:

- **سوشل نیٹ ورکنگ کے فوائد:** سوشل نیٹ ورکنگ پلیٹ فارم ہمیں جڑے رہنے اور معلومات کو تیزی سے شیئر کرنے میں مدد کرتے ہیں۔ مثال کے طور پر، فیس بک صارفین کو دوستوں اور فیملی کے ساتھ رابطے میں رہنے، اپ ڈیٹس شیئر کرنے اور دلچسپی کے گروپوں میں شامل ہونے کی اجازت دیتا ہے۔
- **غلط معلومات کے خطرات:** اگرچہ سوشل میڈیا مفید ہے، لیکن یہ غلط معلومات بھی پھیلا سکتا ہے۔ غلط معلومات لوگوں کو گمراہ کر سکتی ہیں اور الجھن کا باعث بن سکتی ہیں۔ مثال کے طور پر، صحت کے مسئلے کے بارے میں جھوٹی خبریں تیزی سے پھیل سکتی ہیں اور نقصان دہ رویے کا باعث بن سکتی ہیں۔ یقین کرنے یا شیئر کرنے سے پہلے قابل اعتماد ذرائع سے معلومات کی تصدیق کرنا ضروری ہے۔

کمپیوٹنگ سسٹم میں پرائیویسی، سیکیورٹی، اور استعمال کے درمیان تجارت

کمپیوٹنگ سسٹم کو ڈیزائن کرتے اور استعمال کرتے وقت، رازداری، سلامتی اور استعمال کے درمیان تجارت ہوتی ہے:

- **رازداری بمقابلہ استعمال:** بعض اوقات، رازداری کی حفاظت کسی نظام کو استعمال کرنے میں کم آسان بنا سکتی ہے۔ مثال کے طور پر، مضبوط پاس ورڈز اور دو عوامل کی توثیق کی ضرورت لاگ ان کو زیادہ محفوظ بنا سکتی ہے لیکن اس میں زیادہ وقت بھی لگ سکتا ہے۔ استعمال میں آسانی اور مضبوط حفاظتی اقدامات کے درمیان توازن تلاش کرنا ضروری ہے۔
- **سیکیورٹی بمقابلہ افادیت:** اعلیٰ حفاظتی اقدامات کو نافذ کرنا بعض اوقات نظام کو کم صارف دوست بنا سکتا ہے۔ مثال کے طور پر، ایک پیچیدہ حفاظتی نظام صارفین کے لیے نیویگیٹ کرنا مشکل ہو سکتا ہے۔ ایسے نظاموں کو ڈیزائن کرنا ضروری ہے جو محفوظ اور استعمال میں آسان دونوں ہوں، اس بات کو یقینی بناتے ہوئے کہ صارفین سہولت کی قربانی کے بغیر محفوظ ہیں۔

انشائی طرز کنسیپچوئل (Conceptual) سوالات

سوال 1: وضاحت کریں کہ آج کی ڈیجیٹل دنیا میں ذمہ دار کمپیوٹر کا استعمال کیوں اہم ہے۔ بحث کریں کہ مناسب ہارڈ ویئر اور سافٹ ویئر کا انتخاب سیکیورٹی، کارکردگی اور مطابقت کو کس طرح متاثر کرتا ہے۔

جواب: آج کی ڈیجیٹل دنیا میں ذمہ دار کمپیوٹر کا استعمال ضروری ہے کیونکہ یہ ڈیٹا کی حفاظت میں مدد کرتا ہے، ہموار آپریشن کو یقینی بناتا ہے، اور حفاظتی خطرات کو روکتا ہے۔ صحیح ہارڈ ویئر اور سافٹ ویئر کا انتخاب تین اہم وجوہات کی بنا پر اہم ہے:

حفاظت: فرسودہ یا غیر محفوظ سافٹ ویئر کا استعمال وائرس اور ہیکنگ کے خطرے کو بڑھاتا ہے۔ تازہ ترین اینٹی وائرس تحفظ کے بغیر، ذاتی معلومات چوری کی جا سکتی ہیں۔

کارکردگی: ہارڈ ویئر اور سافٹ ویئر کا صحیح امتزاج کام کی فوری تکمیل کو یقینی بناتا ہے۔ مثال کے طور پر، پرانے کمپیوٹر پر جدید ویڈیو گیم چلانے سے یہ پیچھے رہ سکتا ہے یا بالکل کام نہیں کر سکتے۔

مطابقت: سافٹ ویئر اور ہارڈ ویئر کو ہموار آپریشن کے لیے ہم آہنگ ہونا چاہیے۔ نیا سافٹ ویئر انسٹال کرنے سے پہلے، صارفین کو کارکردگی کے مسائل سے بچنے کے لیے سسٹم کی ضروریات کو چیک کرنا چاہیے۔

کمپیوٹر کے استعمال کے حوالے سے سوچ سمجھ کر فیصلے کرنے سے، افراد سلامتی، پیداوری اور مجموعی صارف کے تجربے کو بڑھا سکتے ہیں۔

stepacademyofficial.com

سوال 2: انٹرنیٹ کے ذمہ دارانہ استعمال کی اہمیت اور افراد اور معاشرے پر اس کے اثرات پر بحث کریں۔

جواب: آن لائن حفاظت کو یقینی بنانے، غلط معلومات کو روکنے اور ڈیجیٹل فلاح و بہبود کو برقرار رکھنے کے لیے انٹرنیٹ کا ذمہ دارانہ استعمال ضروری ہے۔ یہ افراد کی رازداری، ذہنی صحت اور آن لائن سیکورٹی کی حفاظت کے ذریعے ان پر اثر انداز ہوتا ہے۔ سماجی سطح پر، ذمہ دارانہ استعمال سائبر کرائم، سائبر غنڈہ گردی اور غلط معلومات کے پھیلاؤ کو روکتا ہے۔

اعتبار کی تشخیص: غلط معلومات سے بچنے کے لیے معلومات کے ذرائع کی تصدیق ضروری ہے۔ متعدد ذرائع کی جانچ کرنا، سنسنی خیز سرخیوں پر شک کرنا، اور تعلیمی (.edu) یا سرکاری (.gov) ویب سائٹوں پر انحصار کرنا درستگی کو یقینی بناتا ہے۔

آن لائن حفاظت: مشکوک لنکس سے گریز کر کے، محفوظ پاس ورڈز کا استعمال کر کے، اور آن لائن معلومات کا اشتراک کرتے وقت محتاط رہنے سے ذاتی ڈیٹا کی حفاظت شناخت کی چوری اور ہیکنگ جیسے خطرات کو کم کرتی ہے۔

ڈیجیٹل فلاح و بہبود: باقاعدہ وقفوں، ذہن میں رکھنے والی ٹیکنالوجی کے استعمال اور اسکرین کے وقت کو کم کرنے کے ذریعے متوازن ڈیجیٹل طرز زندگی کو برقرار رکھنا ذہنی صحت اور پیداوری میں مدد کرتا ہے۔

ان حکمت عملیوں پر عمل کر کے، افراد انٹرنیٹ کو ایک محفوظ اور زیادہ پیداواری جگہ بنا سکتے ہیں۔

سوال 3: کمپیوٹنگ نے انسانی تعاملات، طرز عمل اور سماجی ڈھانچے کو تبدیل کر دیا ہے۔ بحث کریں کہ کس طرح کمپیوٹنگ اخلاقی، ماحولیاتی، قانونی، سماجی، اقتصادی اور ثقافتی اثرات سمیت مختلف پہلوؤں میں طرز عمل اور طریقوں کو متاثر کرتی ہے۔

جواب: کمپیوٹنگ ہماری زندگیوں کے بہت سے پہلوؤں کو متاثر کرتی ہے، ماحول سے لے کر ہمارے ثقافتی طریقوں تک۔ کمپیوٹنگ کے مختلف اثرات میں شامل ہیں:

اخلاقی اثر: کمپیوٹنگ سے اخلاقی خدشات پیدا ہوتے ہیں، جیسے کہ کسی اور کے کام کو اجازت کے بغیر استعمال کرنا، جو کہ غیر اخلاقی ہے۔ کاپی رائٹ کے قوانین کا احترام کرنا ضروری ہے۔

ماحولیاتی اثرات: ٹیکنالوجی ماحولیاتی خدشات جیسے ای۔ فضلہ اور توانائی کی کھپت میں حصہ ڈال سکتی ہے۔

قانونی اثرات: قانونی مسائل میں رازداری کے قوانین اور دانشورانہ املاک کے حقوق شامل ہیں۔ تخلیق کار کو کریڈٹ دیے بغیر ڈیجیٹل مواد کا غیر مجاز استعمال غیر قانونی ہے۔

سماجی اثر: سوشل نیٹ ورکنگ تنظیموں، کاروباروں اور افراد کو آسانی سے بات چیت کرنے میں مدد کرتی ہے۔ تاہم، یہ غلط معلومات اور رازداری کی خلاف ورزیوں کا باعث بھی بن سکتا ہے۔

اقتصادی اثر: کمپیوٹنگ نے نئی صنعتیں اور روزگار کے مواقع پیدا کیے ہیں، جیسے سافٹ ویئر ڈویلپمنٹ اور ڈیجیٹل مارکیٹنگ۔ تاہم، آٹومیشن نے کچھ روایتی کاموں کی جگہ لے لی ہے۔

ثقافتی اثر: کمپیوٹنگ لوگوں کو نئی ٹیکنالوجی اور عالمی منڈیوں کے مطابق ڈھالنے میں مدد کرتی ہے، جس سے ثقافتی تبدیلیاں اور مواصلاتی انداز متاثر ہوتے ہیں۔

دلچسپ معلومات

- آن لائن آداب: ''سنہری اصول'' کا اطلاق آن لائن بھی ہوتا ہے، دوسروں کے ساتھ ویسا ہی سلوک کریں جیسا آپ چاہتے ہیں۔ یہ احترام اور مثبت بات چیت کو برقرار رکھنے میں مدد کرتا ہے۔

stepacademyofficial.com

- **سائبر حفظان صحت:** جراثیم سے بچنے کے لیے اپنے ہاتھ دھونے کی طرح، ڈیجیٹل وائرس سے بچنے کے لیے اپنے اینٹی وائرس سافٹ ویئر کو باقاعدگی سے اپ ڈیٹ کرنا ضروری ہے۔
- **ٹو فیکٹر اتھنٹی فکیشن (2FA):** 2FA کا تصور پہلی بار 1980ء کی دہائی میں استعمال کیا گیا تھا، لیکن یہ 2000ء کی دہائی میں آن لائن اکاؤنٹس کے عروج کے ساتھ وسیع ہو گیا۔
- **سافٹ ویئر اپ ڈیٹس:** مائیکروسافٹ ہر چھ ماہ بعد ونڈوز کے لیے بڑی اپ ڈیٹس جاری کرتا ہے، جس سے یہ ظاہر ہوتا ہے کہ سکیورٹی کے لیے ٹیکنالوجی کو کتنی بار ریفریش کرنے کی ضرورت ہے۔
- **ڈیٹا اکٹھا کرنا:** ''باخبر رضامندی'' کے اخلاقی اصول کا مطلب ہے کہ آپ کو یہ جاننے کا حق ہے کہ آپ کا ڈیٹا کیسے استعمال کیا جا رہا ہے۔ اس اصول پر 2004 کی بائیو ایتھکس کمیشن کی رپورٹ میں زور دیا گیا تھا۔
- **سرچ انجن کے سنگ میل:** گوگل یومیہ 3.5 بلین سے زیادہ تلاشوں پر کارروائی کرتا ہے، جو اسے معتبر معلومات تلاش کرنے کے لیے سب سے مقبول سرچ انجن بناتا ہے۔
- **ڈیٹا کی خلاف ورزی:** 2013ء میں، ڈیٹا کی سب سے بڑی خلاف ورزی نے Yahoo کو متاثر کیا، جس سے 3 بلین اکاؤنٹس کا ڈیٹا بشمول نام، ای میل ایڈریسز اور پاس ورڈ بے نقاب ہوا۔
- **سافٹ ویئر پائریسی کا اثر:** سافٹ ویئر پائریسی کا تخمینہ ہے کہ عالمی معیشت کو سالانہ 46 بلین ڈالر سے زیادہ کی لاگت آئے گی، جو ڈویلپرز اور کاروباروں پر نمایاں اثرات کو ظاہر کرتی ہے۔
- **ساکھ کی جانچ:** ''edu.'' ڈومینز والی ویب سائٹیں عموماً تعلیمی ادارے ہوتی ہیں اور اکثر تحقیق کے لیے زیادہ قابل اعتماد ذرائع ہوتی ہیں۔
- **ٹیکنالوجی کا ارتقاء:** پہلا کمپیوٹر ماؤس، جو 1964 میں ایجاد ہوا، ایک لکڑی کا باکس تھا جس میں ایک بٹن تھا۔ آج کے ماؤس متعدد بٹنوں اور جدید خصوصیات کے ساتھ آتے ہیں!

stepacademyofficial.com

معروضی سوالات

محکمہ تعلیم کی نئی امتحانی تکنیکس (Knowledge, Understanding, Application, Analytical & Conceptual) کی روشنی میں مرتب کیے گئے کثیر الانتخابی سوالات

11.1 کمپیوٹر کا ذمہ دارانہ استعمال

☆ درست جواب کے گرد دائرہ لگائیں۔

-1 صارف کو اپنے کمپیوٹر پر نیا سافٹ ویئر انسٹال کرنے سے پہلے کیا کرنا چاہیے؟

(A) سسٹم کی ضروریات کو چیک کیے بغیر اسے انسٹال کریں

(B) ان کی ہارڈ ویئر کی خصوصیات کے ساتھ مطابقت کی جانچ کریں

(C) اپ ڈیٹس کو نظر انداز کریں اور پرانے ورژن کا استعمال جاری رکھیں

(D) تمام سابقہ سافٹ ویئر کو ہٹا دیں

-2 دیئے گئے متن کے مقابلے میں سائبر حفظان صحت کیا ہے؟

(A) کمپیوٹر اسکرین کو صاف کرنا
(B) جراثیم سے بچنے کے لیے ہاتھ دھونا
(C) پرانی فائلوں کو اسٹوریج سے حذف کرنا
(D) ہارڈ ڈرائیو کو فارمیٹ کرنا

-3 اگر کوئی پرانے کمپیوٹر پر جدید گیم کھیلنے کی کوشش کرتا ہے تو کیا ہوتا ہے؟

(A) کھیل آسانی سے چلے گا
(B) کھیل سست ہو سکتا ہے یا بالکل کام نہیں کر سکتا ہے
(C) کمپیوٹر زیادہ موثر ہو جائے گا
(D) کمپیوٹر خود بخود اپ ڈیٹ ہو جائے گا

11.2 کمپیوٹر کے ذمہ دارانہ استعمال کا جائزہ

-4 اگر کوئی طالب علم سسٹم کی ضروریات کو دیکھے بغیر اکثر ایپلی کیشنز ڈاؤن لوڈ کرتا ہے، تو اسے کس پریشانی کا سامنا کرنا پڑ سکتا ہے؟

(A) مطابقت نہ ہونے کی وجہ سے سافٹ ویئر مناسب طریقے سے کام نہیں کر سکتا ہے
(B) کمپیوٹر کو خود کار حفاظتی اپڈیٹس ملیں گی۔
(C) ایپلی کیشنز توقع سے زیادہ تیزی سے چلیں گی۔
(D) کمپیوٹر کو کبھی بھی اینٹی وائرس تحفظ کی ضرورت نہیں پڑے گی۔

-5 ٹو فیکٹر توثیق (2 ایف اے) کو آن لائن اکاؤنٹس کی حفاظت کا زیادہ محفوظ طریقہ کیوں سمجھا جاتا ہے؟

(A) یہ صارفین کو پاس ورڈ درج کیے بغیر لاگ ان کرنے کی اجازت دیتا ہے۔
(B) اس میں صارفین کو تصدیق کی دوسری شکل درج کرنے کی ضرورت ہوتی ہے، جیسے کہ ان کے فون پر بھیجا گیا کوڈ، جس سے ہیکنگ مشکل ہو جاتی ہے۔
(C) یہ تمام نئے آلات سے اکاؤنٹس تک رسائی کو روکتا ہے۔
(D) یہ پاس ورڈز کو باقاعدگی سے اپ ڈیٹ کرنے کی ضرورت کو دور کرتا ہے۔

-6 حساس لین دین کرتے وقت پبلک وائی فائی سے گریز کرنے کی بنیادی وجہ کیا ہے؟

(A) پبلک وائی فائی کنکشن عام طور پر سست ہوتے ہیں۔
(B) پبلک وائی فائی نیٹ ورک ہیکرز اور غیر مجاز رسائی کے لیے ذاتی ڈیٹا کو بے نقاب کر سکتے ہیں۔
(C) پبلک وائی فائی بینکنگ ویب سائٹس تک رسائی کی اجازت نہیں دیتا ہے۔
(D) پبلک وائی فائی صرف موبائل آلات پر کام کرتا ہے، لیپ ٹاپ پر نہیں۔

-7 باقاعدگی سے سافٹ ویئر اپ ڈیٹس ڈیجیٹل پلیٹ فارم کی حفاظت میں کس طرح حصہ ڈالتے ہیں؟

(A) وہ صارف کے تجربے کو بہتر بنانے کے لیے مزید خصوصیات شامل کرتے ہیں۔
(B) وہ خود بخود نامعلوم صارفین کو اکاؤنٹس تک رسائی سے روک دیتے ہیں۔
(C) وہ حفاظتی خطرات کو ٹھیک کرتے ہیں اور آلات کو سائبر خطرات سے بچاتے ہیں۔
(D) وہ نظام کو تیز اور ہموار بناتے ہیں۔

-8 اگر کسی صارف کو کسی نامعلوم سینڈر کی طرف سے ذاتی بینکنگ کی تفصیلات کے لیے ای میل موصول ہوتی ہے، تو اس کے لیے بہترین طریقہ کار کیا ہے؟

(A) فوری جواب دیں اور مطلوبہ معلومات فراہم کریں۔
(B) فراہم کردہ لنک پر کلک کریں اور چیک کریں کہ آیا ویب سائٹ جائز لگتی ہے۔
(C) ممکنہ دھوکہ دہی کو روکنے کے لیے ای میل کو نظر انداز کریں یا اسے سپیم کے طور پر رپورٹ کریں۔
(D) دوستوں کو ای میل بھیج کر اس بات کی تصدیق کریں کہ آیا انہیں بھی وہی درخواست موصول ہوئی ہے۔

stepacademyofficial.com

11.3 ڈیجیٹل پلیٹ فارمز کا محفوظ اور محفوظ آپریشن

-9 اگر کسی صارف کو کسی نامعلوم سینڈر کی طرف سے منسلک ای میل موصول ہوتی ہے، تو انہیں کیا کرنا چاہیے؟

(A) اس کا مواد چیک کرنے کے لیے اسے فوراً کھولیں (B) جواب دیں اور مزید تفصیلات طلب کریں

(C) ممکنہ خطرات سے بچنے کے لیے اسے نظر انداز کریں یا سپیم کے طور پر نشان زد کریں

(D) اسے تصدیق کے لیے دوستوں کو بھیج دیں

-10 سوشل میڈیا اور ای میل سروسز پر پرائیویسی سیٹنگز کا بنیادی کام کیا ہے؟

(A) انٹرنیٹ کی رفتار بڑھانے کے لیے (B) ایڈجسٹ کرے کہ صارف کی معلومات کون دیکھ سکتا ہے

(C) انٹرنیٹ ہیکنگ کو مکمل طور پر روکنے کے لیے (D) آن لائن اشتہارات کے معیار کو بہتر بنانا

-11 ڈیٹا سیکیورٹی کے اقدامات ذاتی معلومات کی حفاظت میں کس طرح مدد کرتے ہیں؟

(A) مضبوط پاس ورڈز کو یقینی بنا کر اور غیر مجاز رسائی کو محدود کر کے

(B) تمام صارفین کو ذخیرہ شدہ معلومات دیکھنے کی اجازت دے کر

(C) ذخیرہ شدہ ڈیٹا کو خودکار طور پر نظر انداز کر کے (D) کسٹمر سپورٹ کے ساتھ لاگ ان کی اسناد کا اشتراک کر کے

-12 اگر آپ اپنے کلاؤڈ اسٹوریج اکاؤنٹ کو محفوظ کرنا چاہتے ہیں تو آپ کو کیا کرنا چاہیے؟

(A) کمزور اور یاد رکھنے میں آسان پاس ورڈ استعمال کریں

(B) قابل اعتماد دوستوں کے ساتھ لاگ ان معلومات شیئر کریں

(C) مضبوط پاس ورڈ مرتب کریں اور حساس معلومات کو ذخیرہ کرنے سے گریز کریں

(D) مضبوط سافٹ ویئر مرتب کریں اور حساس معلومات کو ذخیرہ کرنے سے گریز کریں

11.4 قانونی اور اخلاقی فریم ورک

-13 اگر کوئی تنظیم صارفین کو بتائے بغیر ذاتی ڈیٹا اکٹھا کرتی ہے، تو وہ کس اخلاقی اصول کی خلاف ورزی کرتی ہے؟

(A) شفافیت (B) منافع بخش (C) مقابلہ (D) رفتار

-14 ڈیٹا اخلاقیات کے کلیدی اخلاقی اصول کیا ہیں؟

(A) شفافیت، رازداری، انصاف پسندی اور احتساب

(B) معلومات کو چھپانا، رسائی کو محدود کرنا، اور ڈیٹا شیئرنگ کو روکنا

(C) منافع کے لیے تیسرے فریق کو ڈیٹا فروخت کرنا (D) تمام ڈیٹا کو عوامی طور پر قابل رسائی بنانا

-15 ذمہ دار ڈیٹا ہینڈلنگ سے افراد اور تنظیموں کو کس طرح فائدہ ہوتا ہے؟

(A) یہ رازداری، سلامتی کو یقینی بناتا ہے، اور اعتماد پیدا کرتا ہے (B) یہ ہر ایک کے لیے ذاتی ڈیٹا تک رسائی میں اضافہ کرتا ہے۔

(C) یہ کمپنیوں کو لامحدود ذاتی معلومات ذخیرہ کرنے کی اجازت دیتا ہے۔

(D) اس سے قانونی ضابطوں کی ضرورت کم ہو جاتی ہے۔

-16 ایک اسکول طلباء کے گریڈ آن لائن شیئر کرنا چاہتا ہے۔ ڈیٹا کی اخلاقی ہینڈلنگ کو یقینی بنانے کے لیے انہیں کیا کرنا چاہیے؟

(A) شفافیت کے لیے تمام طلباء کے گریڈ عوامی طور پر شیئر کریں

stepacademyofficial.com

https://stepacademyofficial.com/

(B) طلباء اور والدین کو مطلع کریں، رضامندی حاصل کریں، اور ڈیٹا کو محفوظ کریں
(C) صرف اندرونی استعمال کے لیے اساتذہ کو گریڈ بھیجیں
(D) تحقیقی مقاصد کے لیے طلباء کے ریکارڈ تک کھلی رسائی کی اجازت دیں۔

11.5 دانشورانہ املاک کے تصورات

-17 **کاروباری اداروں کے لیے یہ کیوں ضروری ہے کہ وہ اپنی مصنوعات کے لیے ٹریڈ مارک استعمال کریں؟**
(A) سافٹ ویئر کی غیر قانونی کاپی کو روکنے کے لیے
(B) برانڈ کی شناخت پیدا کرنا اور صارفین کی الجھن کو روکنا
(C) دوسروں کو اپنے برانڈ کو مارکیٹنگ کے لیے استعمال کرنے کی اجازت دینا
(D) ڈیجیٹل مواد کی پیداواری لاگت کو کم کرنا

-18 **سافٹ ویئر کی پائریسی کو نقصان دہ سمجھے جانے کی بنیادی وجہ کیا ہے؟**
(A) یہ زیادہ سے زیادہ لوگوں کو سافٹ ویئر تک مفت رسائی کی اجازت دیتا ہے
(B) یہ سافٹ ویئر ڈویلپرز کو اپنے کام کے لیے پیسہ کمانے سے روکتا ہے۔
(C) یہ سافٹ ویئر کو وسیع تر سامعین تک پہنچانے میں مدد کرتا ہے۔
(D) یہ سافٹ ویئر کی تقسیم پر قانونی پابندیوں کو کم کرتا ہے

-19 **کاپی رائٹ قانون مصنف کی تحریری کتاب کی حفاظت کیسے کرتا ہے؟**
(A) کتاب کی مفت نقل کی اجازت دے کر
(B) غیر مجاز کاپی، شیئرنگ اور تقسیم کو روک کر
(C) صرف کتابوں کی دکانوں کو حقوق دے کر
(D) پرنٹ کی جانے والی کاپیوں کی تعداد کو محدود کر کے

-20 **ایک کمپنی ایک نیا سافٹ ویئر جاری کرتی ہے اور اسے کاپی رائٹ قانون کے تحت رجسٹر کرتی ہے۔ یہ کمپنی کے حقوق کی حفاظت کیسے کرتا ہے؟**
(A) کمپنی قانونی طور پر غیر مجاز تقسیم اور نقل کو روک سکتی ہے
(B) کمپنی کو سافٹ ویئر مفت میں شیئر کرنا چاہیے
(C) سافٹ ویئر بغیر کسی پابندی کے عوام کے استعمال کے لیے دستیاب ہو جاتا ہے۔
(D) سافٹ ویئر ایک سال کے بعد اپنا قانونی تحفظ کھو دیتا ہے۔

-21 **اگر کوئی طالب علم بغیر ادائیگی کے کسی غیر مجاز ویب سائٹ سے فلم ڈاؤن لوڈ کرتا ہے تو کس قانون کی خلاف ورزی ہو رہی ہے؟**
(A) پیٹنٹ قانون
(B) ٹریڈ مارک کا قانون
(C) کاپی رائٹ قانون
(D) ڈیجیٹل اشتہاری قانون

11.6 ذمہ دار انٹرنیٹ استعمال

-22 **اگر کسی شخص کو انٹرنیٹ کا استعمال بند کرنا مشکل لگتا ہے اور وہ روزمرہ کے کاموں کو نظر انداز کرنا شروع کر دیتا ہے تو اس کے لیے بہترین طریقہ کار کیا ہے؟**
(A) تمام جاری سرگرمیوں کو مکمل کرنے کے لیے اور بھی زیادہ وقت آن لائن گزاریں
(B) باقاعدگی سے وقفے لیں اور آف لائن سرگرمیوں میں مشغول رہیں
(C) متعدد سوشل میڈیا پلیٹ فارمز کا استعمال بڑھائیں
(D) مسئلے کو نظر انداز کریں اور ہمیشہ کی طرح جاری رکھیں

stepacademyofficial.com

-23 غیر واقف یا مشکوک لنکس پر کلک کرتے وقت لوگوں کو محتاط کیوں رہنا چاہیے؟

(A) وہ نقصان دہ ویب سائٹس کا باعث بن سکتی ہیں جو ذاتی معلومات چوری کرتی ہیں۔

(B) وہ پریمیم مواد تک مفت رسائی فراہم کرتے ہیں۔

(C) وہ صارفین کو تفریح کے نئے اختیارات تلاش کرنے میں مدد کرتے ہیں۔

(D) ان کی ہمیشہ سرچ انجنوں کے ذریعے تصدیق کی جاتی ہے۔

-24 کیسے ایک شخص انٹرنیٹ کا استعمال کرتے ہوئے ایک متوازن ڈیجیٹل طرز زندگی کو برقرار رکھ سکتا ہے؟

(A) اپنا سارا فارغ وقت آن لائن گزار کر

(B) بریک لے کر، ٹیکنالوجی کا دانشمندی سے استعمال کر کے، اور ذہنی تندرستی پر توجہ مرکوز کر کے

(C) حفاظتی اقدامات کو نظر انداز کر کے اور آزادانہ طور پر معلومات کا اشتراک کر کے

(D) ڈیجیٹل مواصلات کی تمام شکلوں سے گریز کر کے

-25 اگر کسی فرد کو سائبر غنڈہ گردی کا سامنا کرنا پڑے تو اسے کیا کرنا چاہیے؟

(A) اسے خفیہ رکھیں اور اس پر کسی سے بحث کرنے سے گریز کریں۔ (B) غنڈہ گردی کا جارحانہ انداز میں جواب دیں

(C) واقعے کی اطلاع کسی قابل اعتماد شخص یا اتھارٹی کو دیں (D) ان کے سوشل میڈیا اکاؤنٹس کو فوری طور پر حذف کر دیں

11.7 معاشرے پر کمپیوٹنگ کا اثر

-26 کمپیوٹنگ جدید صنعتوں میں معاشی طریقوں کو کس طرح متاثر کرتی ہے؟

(A) معاشی سرگرمیوں پر اس کا کوئی اثر نہیں پڑتا (B) یہ روایتی ملازمتوں کی جگہ آٹومیشن لے لیتا ہے

(C) یہ صرف چھوٹے پیمانے کے کاروبار کو متاثر کرتا ہے (D) یہ ڈیجیٹل مارکیٹنگ کے استعمال کی حوصلہ شکنی کرتا ہے

-27 اگر سوشل میڈیا پلیٹ فارم غلط معلومات پھیلاتے ہیں تو اس کے منفی اثرات کو کم کرنے کا بہترین طریقہ کیا ہے؟

(A) دوستوں کے ساتھ غیر تصدیق شدہ خبریں شیئر کرنا (B) تمام آن لائن معلومات پر بھروسہ کرنا اور پھیلانا

(C) شیئر کرنے سے پہلے قابل اعتماد ذرائع سے معلومات کی تصدیق کرنا

(D) تمام قسم کے آن لائن مواصلات سے گریز کرنا۔

-28 سوشل نیٹ ورکنگ پلیٹ فارم کا ایک بڑا فائدہ کیا ہے؟

(A) وہ عالمی مواصلات میں رکاوٹیں پیدا کرتے ہیں

(B) وہ لوگوں کو جڑے رہنے اور معلومات کو تیزی سے بانٹنے میں مدد کرتے ہیں۔

(C) وہ آئی ٹی صنعتوں میں روزگار کے مواقع کو کم کرتے ہیں (D) وہ غلط معلومات کے تمام خطرات کو ختم کرتے ہیں۔

-29 کون سا اہم عنصر ہے جو کمپیوٹنگ ڈرائیو کلچرل ارتقاء میں مدد کرتا ہے؟

(A) روایتی خط پر مبنی مواصلات (B) عالمی تعامل کے لیے آن لائن پلیٹ فارم

(C) ڈیجیٹل لین دین پر پابندی (D) تعلیم میں ٹیکنالوجی کے استعمال کو محدود کرنا

-30 کمپیوٹنگ سسٹم ڈیزائن کرتے وقت درج ذیل میں سے کون سا ٹریڈ آف ہے؟

(A) رازداری، سلامتی اور استعمال کے قابل ہونے میں توازن (B) کمپیوٹنگ آلات کی لاگت میں اضافہ

(C) استعمال کو نظر انداز کرتے ہوئے صرف تحفظ کو یقینی بنانا (D) کمپیوٹنگ کو عالمی صارفین کے لیے ناقابل رسائی بنانا

stepacademyofficial.com

(B) -10	(C) -9	(C) -8	(C) -7	(B) -6	(B) -5	(A) -4	(B) -3	(B) -2	(B) -1
(A) -20	(B) -19	(B) -18	(B) -17	(B) -16	(A) -15	(A) -14	(A) -13	(C) -12	(A) -11
(A) -30	(B) -29	(B) -28	(C) -27	(B) -26	(C) -25	(B) -24	(A) -23	(B) -22	(C) -21

کثیر الانتخابی کنسیپچوئل (Conceptual) سوالات

☆ درست جواب کے گرد دائرہ لگائیں۔

-1 کمپیوٹر کے ذمہ دارانہ استعمال کے لیے صحیح ہارڈ ویئر اور سافٹ ویئر کا انتخاب کیوں ضروری ہے؟

(A) یہ کمپیوٹر کے سائز کو بڑھانے میں مدد کرتا ہے
(B) یہ حفاظت، کارکردگی اور مطابقت کو بہتر بناتا ہے
(C) یہ کمپیوٹر کو بجلی کے بغیر کام کرواتا ہے۔
(D) یہ نظام کو سست کر دیتا ہے

-2 فرسودہ سافٹ ویئر کمپیوٹر کی سلامتی کو کس طرح متاثر کرتا ہے؟

(A) یہ کمپیوٹر کے فنکشن کو تیزی سے سست کرتا ہے
(B) یہ سائبر خطرات کے امکانات کو کم کرتا ہے
(C) اس سے وائرس اور ہیکنگ کا خطرہ بڑھ جاتا ہے
(D) یہ سسٹم کی مطابقت کو بہتر بناتا ہے

-3 مندرجہ ذیل میں سے کون سا بیان ڈیجیٹل پلیٹ فارمز کے لیے مضبوط پاس ورڈ کے استعمال کی اہمیت کی بہترین وضاحت کرتا ہے؟

(A) مضبوط پاس ورڈ صارفین کو اپنے لاگ ان کی تفصیلات کو آسانی سے یاد رکھنے میں مدد کرتے ہیں۔
(B) مضبوط پاس ورڈ اکاؤنٹس کو غیر مجاز رسائی سے بچاتے ہیں جس سے ہیکرز کے لیے اندازہ لگانا مشکل ہو جاتا ہے۔
(C) مضبوط پاس ورڈز کا استعمال آن لائن اکاؤنٹس تک تیزی سے رسائی کو یقینی بناتا ہے۔
(D) مضبوط پاس ورڈ انٹرنیٹ کی رفتار میں اضافہ کرتے ہیں۔

-4 سوشل میڈیا، ای میل، کلاؤڈ سروسز، اور آن لائن ایپلی کیشنز کو ذمہ داری کے ساتھ استعمال کرنے کی بنیادی وجہ کیا ہے؟

(A) آن لائن سرگرمی کو بڑھانا
(B) ذاتی تحفظ اور ڈیٹا کی حفاظت کو یقینی بنانا
(C) سوشل میڈیا پر مزید پیروکار حاصل کرنے کے لیے
(D) مفت مواد تک آسانی سے رسائی حاصل کرنا

-5 ذاتی معلومات جیسے گھر کا پتہ یا فون نمبر سوشل میڈیا پر شیئر کرنے سے گریز کرنا کیوں ضروری ہے؟

(A) یہ رازداری کے خطرات اور سائبر خطرات کا باعث بن سکتا ہے
(B) اس سے زیادہ لائیکس اور فالوورز حاصل کرنے میں مدد ملتی ہے
(C) یہ کمپنیوں کو بہتر تشہیر کرنے کی اجازت دیتا ہے
(D) اس سے بات چیت آسان ہو جاتی ہے

-6 ڈیجیٹل دنیا میں پرائیویسی قوانین کا بنیادی مقصد کیا ہے؟

(A) انٹرنیٹ کے استعمال کو محدود کرنا
(B) ذاتی ڈیٹا کو غلط استعمال اور غیر مجاز رسائی سے بچانے کے لئے
(C) ذاتی ڈیٹا کے آزادانہ تبادلے کو فروغ دینا
(D) کمپنیوں کو ذاتی ڈیٹا کو آزادانہ طور پر استعمال کرنے کی اجازت دینا

stepacademyofficial.com

https://stepacademyofficial.com/

7- کمپنیوں کے لیے ڈیٹا کے تحفظ کی ذمہ داری لینا کیوں ضروری ہے؟

(A) اپنے کاروباری منافع میں اضافہ کرنا
(B) سزاؤں اور قانونی نتائج سے بچنے کے لیے
(C) تیسرے فریق کے ساتھ صارفین کا ڈیٹا شیئر کرنا۔
(D) ذاتی ڈیٹا تک آسان رسائی کی اجازت دینا

8- مندرجہ ذیل میں سے کون سا دانشورانہ املاک کے حقوق کے بنیادی مقصد کی بہترین وضاحت کرتا ہے؟

(A) تخلیقی کاموں کی مفت تقسیم کی اجازت دینا
(B) اختراع اور مسابقت کو محدود کرنا
(C) افراد اور تنظیموں کی تخلیقات اور نظریات کا تحفظ کرنا۔
(D) اس بات کو یقینی بنانا کہ صرف کاروبار دانشورانہ املاک کا استعمال کر سکتے ہیں

9- کاروباری اداروں کے لیے یہ کیوں ضروری ہے کہ وہ اپنی مصنوعات کے لیے ٹریڈ مارک استعمال کریں؟

(A) سافٹ ویئر کی غیر قانونی کاپی کو روکنے کے لیے
(B) برانڈ کی شناخت پیدا کرنا اور صارفین کی الجھن کو روکنا
(C) دوسروں کو اپنے برانڈ کو مارکیٹنگ کے لیے استعمال کرنے کی اجازت دینا
(D) ڈیجیٹل مواد کی پیداواری لاگت کو کم کرنا

10- آن لائن معلومات تلاش کرتے وقت ساکھ کی تشخیص کیوں اہم ہے؟

(A) یہ معلومات کی درستگی کی تصدیق میں مدد کرتا ہے۔
(B) یہ صارفین کو تمام ویب سائٹس پر یکساں طور پر بھروسہ کرنے کی اجازت دیتا ہے۔
(C) یہ معلومات کے لیے صرف سوشل میڈیا پر انحصار کرنے کی حوصلہ افزائی کرتا ہے۔
(D) یہ کراس چیکنگ ڈیٹا کی ضرورت کو ختم کرتا ہے۔

11- سوشل نیٹ ورکنگ سیفٹی اور آن لائن آداب سے متعلق کلیدی اخلاقی تشویش کیا ہے؟

(A) پرائیویسی کی ترتیبات کو عوامی رسائی میں ایڈجسٹ کرنا
(B) ذاتی معلومات کا کھلے عام اشتراک
(C) دوسروں کا احترام کرنا اور سائبر بلنگ سے گریز کرنا
(D) آن لائن دھمکیوں اور جارحانہ پیغامات کو نظر انداز کرنا

12- ٹیکنالوجی کے استعمال سے متعلق کمپیوٹنگ میں کلیدی اخلاقی تشویش کیا ہے؟

(A) اجازت کے بغیر کاپی رائٹ والے مواد کا استعمال کرنا
(B) مواصلات کے لیے سوشل میڈیا کا استعمال
(C) آن لائن پلیٹ فارم سے سامان خریدنا
(D) کاروباری عمل کو خودکار بنانا

13- کمپیوٹنگ جدید صنعتوں میں اقتصادی طریقوں پر اثر انداز کرتا ہے؟

(A) معاشی سرگرمیوں پر اس کا کوئی اثر نہیں پڑتا
(B) یہ روایتی ملازمتوں کی جگہ آٹومیشن لے لیتا ہے
(C) یہ صرف چھوٹے پیمانے کے کاروبار کو متاثر کرتا ہے
(D) یہ ڈیجیٹل مارکیٹنگ کے استعمال کی حوصلہ شکنی کرتا ہے

جوابات

-1	(B)	-2	(C)	-3	(B)	-4	(B)	-5	(A)	-6	(B)	-7	(B)
-8	(C)	-9	(B)	-10	(A)	-11	(C)	-12	(A)	-13	(B)		

stepacademyofficial.com

11.1 کمپیوٹر کا ذمہ دارانہ استعمال

11.2 کمپیوٹر کے ذمہ دارانہ استعمال کا جائزہ

☆ مختصر جواب دیں۔

-1 صحیح ہارڈ ویئر اور سافٹ ویئر کا انتخاب کمپیوٹر کے استعمال کے مجموعی تجربے میں کس طرح معاون ہے؟ حفاظت، کارکردگی اور مطابقت کے حوالے سے وضاحت کریں۔

جواب: صحیح ہارڈ ویئر اور سافٹ ویئر کا انتخاب مجموعی کمپیوٹر کے تجربے کو تین طریقوں سے بہتر بناتا ہے:

حفاظت: پرانی یا غیر محفوظ ہارڈ ویئر/سافٹ ویئر وائرس اور ہیکرز کی معلومات چوری کرنے کے خطرے کو بڑھاتا ہے۔

کارکردگی: مناسب ہارڈ ویئر اور سافٹ ویئر کاموں کو تیزی سے مکمل کرنے میں مدد کرتے ہیں۔ مثال کے طور پر، پرانے کمپیوٹر پر نیا ویڈیو گیم چلانے سے تاخیر یا ناکامی ہو سکتی ہے۔

مطابقت: ہارڈ ویئر اور سافٹ ویئر کو ایک ساتھ اچھی طرح سے کام کرنا چاہیے۔ سافٹ ویئر انسٹال کرنے سے پہلے سسٹم کی ضروریات کی جانچ کرنا مناسب مطابقت کو یقینی بناتا ہے۔

11.3 ڈیجیٹل پلیٹ فارمز کا محفوظ اور محفوظ آپریشن

-2 ڈیجیٹل پلیٹ فارمز اور آلات کے 'محفوظ آپریشن' کا کیا مطلب ہے؟ آج کی ڈیجیٹل دنیا میں یہ کیوں ضروری ہے؟

جواب: ڈیجیٹل پلیٹ فارمز اور آلات کے 'محفوظ آپریشن' سے مراد انہیں اس طرح سے استعمال کرنا ہے جو صارفین کو نقصان سے بچاتا ہے اور حفاظتی خطرات سے بچاتا ہے۔ یہ آج کی ڈیجیٹل دنیا میں ضروری ہے کیونکہ آن لائن پلیٹ فارم کا استعمال مواصلات، سیکھنے، تفریح اور کام کے لیے کیا جاتا ہے، جس سے ذاتی معلومات کی حفاظت اور ایک محفوظ آن لائن ماحول کو یقینی بنانا ضروری ہو جاتا ہے۔

-3 نامعلوم لنکس پر کلک کرنے اور غیر معتبر ذرائع سے فائلیں ڈاؤن لوڈ کرنے کے خطرات کیا ہیں؟

جواب: نامعلوم لنکس پر کلک کرنا اور غیر بھروسہ مند ذرائع سے فائلیں ڈاؤن لوڈ کرنا کسی ڈیوائس میں نقصان دہ سافٹ ویئر (میلویئر) متعارف کرا سکتا ہے۔ میلویئر ذاتی معلومات چوری کر سکتا ہے یا نظام کو نقصان پہنچا سکتا ہے، جس سے سیکورٹی کو نقصان پہنچ سکتا ہے۔

-4 رازداری کی ترتیبات صارفین کو ڈیجیٹل پلیٹ فارم پر اپنی ذاتی معلومات کو کنٹرول کرنے میں کس طرح مدد کر سکتی ہیں؟

جواب: رازداری کی ترتیبات صارفین کو یہ منظم کرنے کی اجازت دیتی ہیں کہ کون ان کی ذاتی معلومات دیکھ سکتا ہے اور ان کے ساتھ آن لائن بات چیت کر سکتا ہے۔ ان ترتیبات کو ایڈجسٹ کر کے، صارفین اجنبیوں کی نمائش کو محدود کر سکتے ہیں اور ان کے ڈیٹا تک غیر مجاز رسائی کو روک سکتے ہیں۔ مثال کے طور پر Facebook یا Instagram جیسے سوشل میڈیا پلیٹ فارمز پر آپ یہ انتخاب کر سکتے ہیں۔

-5 دوستوں کے ساتھ اپ ڈیٹس شیئر کرتے وقت بھی ذاتی معلومات کو آن لائن شیئر کرنے سے گریز کرنا کیوں ضروری ہے؟

جواب: اوور شیئرنگ سے گریز کرنا اہم ہے کیونکہ ذاتی تفصیلات جیسے گھر کے پتے، فون نمبر، یا اسکول کے نام شیئر کرنے سے صارفین کو شناختی چوری اور سائبر اسٹاکنگ جیسے حفاظتی خطرات کا سامنا کرنا پڑ سکتا ہے۔ یہاں تک کہ دوستوں کے ساتھ اپ ڈیٹس شیئر کرتے وقت بھی، اگر یہ غلط ہاتھوں میں پڑ جاتی ہے تو اس معلومات کا غلط استعمال ہو سکتا ہے۔

stepacademyofficial.com

6- آپ کیفے میں عوامی وائی فائی استعمال کر رہے ہیں اور آپ کو اپنا بینک اکاؤنٹ چیک کرنے کی ضرورت ہے۔ اِس میں سیکیورٹی کے کون سے خطرات شامل ہیں، اور آپ اپنی معلومات کی حفاظت کیسے کر سکتے ہیں؟

جواب: عوامی وائی فائی اکثر غیر محفوظ ہوتا ہے اور صارفین کو ہیکنگ اور ڈیٹا چوری سے بے نقاب کر سکتا ہے۔ معلومات کی حفاظت کے لیے، صارفین کو عوامی نیٹ ورکس پر حساس لین دین سے گریز کرنا چاہیے، ایک محفوظ نجی نیٹ ورک کا استعمال کرنا چاہیے، اور اضافی سیکیورٹی کے لیے ٹو فیکٹر اتھینٹی فکیشن (2FA) کو فعال کرنا چاہیے۔

7- ڈیٹا کی حفاظت کے اقدامات کیوں ضروری ہیں، اور وہ غیر مجاز رسائی کو روکنے میں کس طرح مدد کر سکتے ہیں؟

جواب: ڈیٹا کی حفاظت کے اقدامات ذاتی معلومات کو سائبر خطرات سے بچانے میں مدد کرتے ہیں۔ مضبوط، منفرد پاس ورڈز کا استعمال اور آن لائن اکاؤنٹس کو محفوظ بنانا ہیکنگ اور ڈیٹا کی خلاف ورزیوں کے خطرے کو کم کرتا ہے۔

8- سیکورٹی کو یقینی بنانے کے لیے ای میل کا استعمال کرتے وقت کیا احتیاطی تدابیر اختیار کی جانی چاہئیں؟

جواب: نامعلوم فرد کی طرف سے بھیجے جانے والی ای میلز کھولتے وقت صارفین کو محتاط رہنا چاہیے، کیونکہ ان میں نقصان دہ لنکس یا اٹیچمنٹ ہو سکتے ہیں۔ فشنگ سکیم سے بچنے اور محفوظ پاس ورڈز کا استعمال ای میل کی حفاظت کو بڑھا سکتا ہے۔

9- صارفین کو سوشل میڈیا پلیٹ فارمز پر ذاتی معلومات شیئر کرنے سے کیوں گریز کرنا چاہیے؟

جواب: ذاتی معلومات کا اشتراک، جیسے گھر کے پتے یا فون نمبر، عوامی طور پر رازداری کے خطرات، شناخت کی چوری، اور سائبر خطرات کا باعث بن سکتے ہیں۔

10- کلاؤڈ سروسز صارفین کے لیے کس طرح فائدہ مند اور خطرناک دونوں ہو سکتی ہیں؟

جواب: کلاؤڈ سروسز اسٹوریج اور فائل شیئرنگ کے آسان اختیارات فراہم کرتی ہیں، لیکن اگر سمجھداری سے استعمال نہ کیا جائے تو وہ خطرات بھی پیدا کرتی ہیں۔ کمزور پاس ورڈ یا حساس معلومات کا اشتراک ڈیٹا کی خلاف ورزیوں کا باعث بن سکتا ہے۔

11- اگر آپ اپنے آن لائن شاپنگ اکاؤنٹ کو محفوظ بنانا چاہتے ہیں تو آپ کو اپنے ڈیٹا کی حفاظت کے لیے کیا اقدامات کرنے چاہئیں؟

جواب: مجھے مضبوط پاس ورڈ استعمال کرنا چاہیے، دو فیکٹر توثیق کو فعال کرنا چاہیے، اور غیر مجاز رسائی کو روکنے کے لیے آن لائن پلیٹ فارم پر مالی تفصیلات کو محفوظ کرنے سے گریز کرنا چاہیے۔

11.4 قانونی اور اخلاقی فریم ورک

12- ڈیٹا کی رازداری کو برقرار رکھنے میں کمپنیوں کے کردار اور اگر وہ ایسا کرنے میں ناکام رہتے ہیں تو انہیں جن نتائج کا سامنا کرنا پڑ سکتا ہے ان کی وضاحت کریں۔

جواب: کمپنیاں ذاتی ڈیٹا اکٹھا اور ذخیرہ کرتی ہیں، انہیں اس کی حفاظت کا ذمہ دار بناتی ہیں۔ اگر وہ اس کی حفاظت کرنے میں ناکام رہتے ہیں تو انہیں قانونی نتائج، صارفین کے اعتماد کے نقصان اور مالی سزاؤں کا سامنا کرنا پڑ سکتا ہے۔ ڈیٹا کی خلاف ورزیوں کو روکنے کے لیے اخلاقی ذمہ داری اور ڈیٹا پروٹیکشن قوانین کی تعمیل بہت ضروری ہے۔

13- آج کے ڈیجیٹل دور میں ڈیٹا اخلاقیات کیوں اہم ہے، اور یہ ڈیٹا کے منصفانہ اور ذمہ دارانہ استعمال کو کیسے یقینی بناتا ہے؟

جواب: ڈیٹا اخلاقیات ذاتی ڈیٹا کو سنبھالتے وقت شفافیت، رازداری کا احترام، انصاف پسندی اور جواب دہی کو یقینی بناتی ہے۔ یہ معلومات کے غلط استعمال کو روکتا ہے، افراد کے حقوق کی حفاظت کرتا ہے، اور صارفین اور تنظیموں کے درمیان اعتماد پیدا کرتا ہے۔

stepacademyofficial.com

https://stepacademyofficial.com/

14- ڈیٹا اکٹھا کرنے اور اشتراک کرنے میں کچھ اخلاقی تحفظات کیا ہیں؟

جواب: اخلاقی تحفظات میں شفافیت، محفوظ ڈیٹا اسٹوریج، اشتراک کرنے سے پہلے صارف کی رضامندی حاصل کرنا، اور یہ یقینی بنانا کہ ذاتی معلومات کا غیر مجاز جماعتوں کے ذریعہ غلط استعمال یا رسائی نہ ہو۔

15- ذمہ دار ڈیٹا ہینڈلنگ افراد اور تنظیموں کو کس طرح متاثر کرتی ہے؟

جواب: ذمہ دار ڈیٹا ہینڈلنگ ذاتی رازداری کی حفاظت کرتا ہے، ڈیٹا کے غلط استعمال کو روکتا ہے، تنظیموں میں اعتماد کو یقینی بناتا ہے، اور قانونی اور اخلاقی معیارات کی تعمیل میں مدد کرتا ہے۔

16- خطوط اسکولوں یا کام کی جگہوں پر ڈیٹا کے اشتراک کے طریقے کو کس طرح متاثر کرتے ہیں؟

جواب: اخلاقی رہنما خطوط اس بات کو یقینی بناتے ہیں کہ اسکولوں یا کام کی جگہوں پر شیئر کیا جانے والا ڈیٹا رضامندی، شفافیت اور مناسب تحفظ کے ساتھ کیا جائے۔ مثال کے طور پر، طلباء کے گریڈ والدین کے ساتھ شیئر کیے جا سکتے ہیں لیکن عوامی طور پر نہیں، رازداری اور انصاف پسندی کو یقینی بناتے ہیں۔

1- فرض کریں کہ کوئی اسکول طلباء کی کارکردگی کی رپورٹیں آن لائن شیئر کرنا چاہتا ہے۔ ایسا کرنے سے پہلے انہیں کن اخلاقی اصولوں پر عمل کرنا چاہیے؟

اب: اسکول کو والدین کی رضامندی حاصل کرنی چاہیے، ڈیٹا کی حفاظت کو یقینی بنانا چاہیے، صرف مجاز افراد کے ساتھ رپورٹس کا اشتراک کرنا چاہیے، اور اعداد و شمار کے اخلاقی اور قانونی تحفظ کے معیارات پر عمل کرتے ہوئے اس کے استعمال کے بارے میں شفاف ہونا چاہیے۔

11.5 دانشورانہ املاک کے تصورات

18- سافٹ ویئر پائریسی کیا ہے، اور اسے غیر قانونی کیوں سمجھا جاتا ہے؟

جواب: سافٹ ویئر کی پائریسی سافٹ ویئر کی غیر قانونی کاپی، تقسیم یا استعمال ہے۔ اسے غیر قانونی سمجھا جاتا ہے کیونکہ سافٹ ویئر خریدار اسے استعمال کرنے کے لیے لائسنس خریدتے ہیں، نہ کہ خود سافٹ ویئر۔ اجازت کے بغیر اس کی نقل اور اشتراک کاپی رائٹ قانون کی خلاف ورزی ہے اور ڈویلپرز کو مالی نقصان پہنچاتا ہے۔

19- سافٹ ویئر کی پائریسی عالمی معیشت کو کس طرح متاثر کرتی ہے؟

جواب: سافٹ ویئر کی پائریسی سے سالانہ 46 ارب ڈالر سے زیادہ کا تخمینہ نقصان ہوتا ہے، جو ڈویلپرز اور کاروباروں کو ان کی آمدنی کو کم کر کے اور جدت طرازی میں رکاوٹ ڈال کر منفی طور پر متاثر کرتا ہے۔

20- ٹریڈ مارک برانڈ کی شناخت میں کیوں اہم کردار ادا کرتے ہیں، اور وہ صارفین میں الجھن کو کیسے روکتے ہیں؟

جواب: ٹریڈ مارک برانڈ کی پہچان کو یقینی بناتے ہوئے کمپنی کی مصنوعات یا خدمات کو دوسروں سے ممتاز کرنے میں مدد کرتے ہیں۔ وہ دوسرے کاروباروں کو اسی طرح کے ناموں، لوگوز یا علامتوں کے استعمال سے منع کر کے، برانڈ پر اعتماد اور وفاداری کو برقرار رکھتے ہوئے صارفین میں الجھن کو روکتے ہیں۔

21- فرض کریں کہ آپ نے کوئی کتاب لکھی ہے اور اسے غیر مجاز نقل سے بچانا چاہتے ہیں۔ آپ کس قسم کا دانشورانہ املاک کا حق استعمال کریں گے، اور کیوں؟

جواب: میں کاپی رائٹ کا استعمال کروں گا کیونکہ اس سے مجھے یہ کنٹرول کرنے کا قانونی حق ملتا ہے کہ میری کتاب کس طرح شائع کی جاتی ہے، شیئر کی جاتی ہے، یا موافقت کی جاتی ہے۔ یہ اس بات کو یقینی بناتا ہے کہ کوئی بھی میری اجازت کے بغیر میری کتاب کی کاپی یا تقسیم نہیں کر سکتا۔

stepacademyofficial.com

22- وضاحت کریں کہ دانشورانہ املاک کے حقوق افراد اور تنظیموں کی تخلیق اور نظریات کے تحفظ میں کس طرح حصہ ڈالتے ہیں۔

جواب: دانشورانہ املاک کے حقوق افراد اور تنظیموں کی تخلیقات اور نظریات کی حفاظت کرتے ہیں اور انہیں یہ اختیار دیتے ہیں کہ ان کے کام کو کس طرح استعمال کیا جاتا ہے۔ یہ اس بات کو یقینی بناتا ہے کہ ان کی فکری کوششیں، جیسے موسیقی، کتابیں، یا ایجادات، بغیر اجازت کے نقل یا تقسیم نہیں کی جائیں گی۔

11.6 ذمہ دار انٹرنیٹ استعمال

23- انٹرنیٹ استعمال کرتے وقت ذاتی معلومات کی حفاظت کے لیے کیا اقدامات کیے جا سکتے ہیں؟

جواب: (i) غیر معتبر ویب سائٹس پر حساس ڈیٹا شیئر کرنے سے گریز کریں۔

(ii) لنکس پر کلک کرتے وقت یا اٹیچمنٹ ڈاؤن لوڈ کرتے وقت محتاط رہیں۔

(iii) مضبوط پاس ورڈ استعمال کریں اور پرائیویسی سیٹنگز کو فعال کریں۔

(iv) ذاتی تفصیلات درج کرنے سے پہلے ویب سائٹ کی ساکھ کی تصدیق کریں۔

24- انٹرنیٹ کا باقاعدگی سے استعمال کرتے ہوئے ڈیجیٹل فلاح و بہبود کو کیسے برقرار رکھا جا سکتا ہے؟

جواب: (i) اسکرینوں سے باقاعدگی سے بریک لیں۔

(ii) سوشل میڈیا اور گیمنگ پر حدود طے کر کے ٹیکنالوجی کا دانشمندی سے استعمال کریں۔

(iii) آن لائن اور آف لائن سرگرمیوں میں توازن رکھ کر ذہنی صحت کو ترجیح دیں۔

(iv) مسلسل اطلاعات جیسی پریشانیوں سے بچیں۔

25- مشکوک لنکس پر کلک کرنے کے خطرات کیا ہیں، اور صارفین اس طرح کے جال میں پڑنے سے کیسے بچ سکتے ہیں؟

جواب: مشکوک لنکس پر کلک کرنے سے فشنگ حملے، میلویئر انفیکشن اور ڈیٹا چوری ہو سکتا ہے۔ صارفین اس طرح کے خطرات سے بچ سکتے ہیں:

(i) ای میلز یا پیغامات میں نامعلوم لنکس پر کلک نہ کریں۔

(ii) صداقت کے لیے یو آر ایل کی جانچ کرنا۔

(iii) اضافی تحفظ کے لیے اینٹی وائرس سافٹ ویئر کا استعمال۔

26- اگر کوئی سائبر غنڈہ گردی کا سامنا کر رہا ہے تو اسے اپنی حفاظت کے لیے کیا اقدامات کرنے چاہئیں؟

جواب: (i) غنڈہ گردی کا جواب نہ دیں۔

(ii) پلیٹ فارم پر موجود شخص کو بلاک کریں اور رپورٹ کریں۔

(iii) مستقبل کے حوالہ کے لیے ثبوت (اسکرین شاٹس، پیغامات) محفوظ کریں۔

(iv) کسی قابل اعتماد بالغ، استاد، یا سائبر کرائم اتھارٹی کو مطلع کریں۔

11.7 معاشرے پر کمپیوٹنگ کا اثر

27- عالمی تجارت اور ثقافتی ارتقاء میں کمپیوٹنگ کے کردار کی وضاحت کریں۔

جواب: کمپیوٹنگ نے عالمی تجارت اور ثقافتی تعاملات کو تبدیل کر دیا ہے:

ایمیزون اور دراز جیسے آن لائن شاپنگ پلیٹ فارمز کو فعال کرنا۔

ڈیجیٹل لین دین اور انوینٹری مینجمنٹ کو آسان بنانا۔

ای میلز، میسجنگ اور سوشل میڈیا کے ذریعے مواصلات کی حمایت کرنا۔

یوٹیوب جیسے ویڈیو پلیٹ فارم کے ذریعے ثقافتی تبادلے میں مدد کرنا۔

stepacademyofficial.com

28- کمپیوٹنگ میں کون سے اخلاقی مسائل پیدا ہوتے ہیں، اور کاپی رائٹ کا احترام کیوں اہم ہے؟

جواب: اخلاقی مسائل میں رازداری کے خدشات اور ڈیجیٹل مواد کا غیر مجاز استعمال شامل ہیں۔ کاپی رائٹ کا احترام اس بات کو یقینی بناتا ہے کہ تخلیق کاروں کو کریڈٹ ملے اور دانشورانہ املاک کے حقوق کا تحفظ ہو۔

29- سوشل نیٹ ورکنگ کے فوائد اور خطرات کیا ہیں؟

جواب: فوائد: لوگوں کو جڑے رہنے اور معلومات کو تیزی سے شیئر کرنے میں مدد کرتا ہے۔

خطرات: غلط معلومات تیزی سے پھیل سکتی ہیں، جس سے الجھن اور غلط عقائد پیدا ہو سکتے ہیں۔

30- سوشل میڈیا پر غلط معلومات معاشرے کو کس طرح متاثر کرتی ہیں؟

جواب: غلط معلومات لوگوں کو گمراہ کر سکتی ہیں، خوف و ہراس پیدا کر سکتی ہیں، اور جھوٹے بیانیے پھیلا سکتی ہیں، جس سے شیئر کرنے سے پہلے قابل اعتماد ذرائع سے معلومات کی تصدیق کرنا ضروری ہو جاتا ہے۔

31- کمپیوٹنگ سسٹم میں پرائیویسی، سیکورٹی اور استعمال کے قابل ہونے میں توازن رکھنا کیوں ضروری ہے؟

جواب: رازداری: صارف کے ڈیٹا کو غیر مجاز رسائی سے محفوظ کرتا ہے۔

تحفظ: سائبر خطرات سے تحفظ کو یقینی بناتا ہے۔

افادیت: نظام تک آسان اور موثر رسائی کی اجازت دیتا ہے۔

توازن: اس بات کو یقینی بناتا ہے کہ نظام صارفین کے لیے بہت پیچیدہ ہوئے بغیر محفوظ رہے۔

32- سوشل نیٹ ورکنگ کے منفی اثرات کو کم کرنے کے لیے افراد کیا اقدامات کر سکتے ہیں؟

جواب: شیئر کرنے سے پہلے معلومات کی تصدیق کریں۔

رازداری کی ترتیبات سے آگاہ رہیں۔

جعلی خبروں کی شناخت کرنے کے لیے خود کو تعلیم دیں۔

مختصر جوابی کنسیپچوئل (Conceptual) سوالات

☆ مختصر جواب دیں۔

1- سائبر حفظان صحت کیا ہے، اور اس کا موازنہ ہاتھ دھونے سے کیوں کیا جاتا ہے؟

جواب: سائبر حفظان صحت سے مراد ڈیجیٹل وائرس سے تحفظ کے لیے اینٹی وائرس سافٹ ویئر کو باقاعدگی سے اپ ڈیٹ کرنا ہے۔ اس کا موازنہ ہاتھ دھونے سے کیا جاتا ہے کیونکہ جس طرح ہاتھ دھونے سے جراثیم کو روکا جاتا ہے، اسی طرح اینٹی وائرس سافٹ ویئر کو اپ ڈیٹ کرنا سائبر خطرات کو روکتا ہے اور نظام کو محفوظ رکھتا ہے۔

2- ٹو فیکٹر اتھنٹی فکیشن (2 ایف اے) آن لائن سیکیورٹی کو کس طرح بڑھاتی ہے، اور یہ 2000 کی دہائی میں بڑے پیمانے پر کیوں استعمال ہوا ہے؟

جواب: ٹو فیکٹر اتھنٹی فکیشن (2 ایف اے) پاس ورڈ درج کرنے کے بعد تصدیق کے اضافی مرحلے، جیسے فون پر بھیجے گئے کوڈ کی ضرورت کے ذریعہ اکاؤنٹس میں ایک اضافی حفاظتی پرت کا اضافہ کرتی ہے۔ یہ 2000 کی دہائی میں آن لائن اکاؤنٹس کے عروج اور سائبر خطرات میں اضافے کی وجہ سے بڑے پیمانے پر استعمال ہونے لگا۔

3- ڈیجیٹل سیکورٹی کے لیے باقاعدگی سے سافٹ ویئر اپ ڈیٹس کیوں اہم ہیں؟ مائیکروسافٹ ونڈوز کے لیے کتنی بار بڑی اپ ڈیٹس جاری کرتا ہے؟

جواب: باقاعدگی سے سافٹ ویئر اپ ڈیٹس اہم ہیں کیونکہ وہ حفاظتی اصلاحات فراہم کرتے ہیں جو آلات کو سائبر خطرات سے بچاتے ہیں۔ مائیکروسافٹ ہر چھ ماہ بعد ونڈوز کے لیے بڑی اپ ڈیٹس جاری کرتا ہے تاکہ یہ یقینی بنایا جا سکے کہ سسٹم محفوظ رہے۔

stepacademyofficial.com

https://stepacademyofficial.com/

4- سوشل میڈیا، ای میل، کلاؤڈ سروسز اور آن لائن ایپلی کیشنز کو ذمہ داری کے ساتھ استعمال کرنا کیوں ضروری ہے؟

جواب: ذاتی حفاظت، ڈیٹا کی حفاظت اور آن لائن اخلاقی رویے کو یقینی بنانے کے لیے ان ڈیجیٹل پلیٹ فارمز کا ذمہ داری سے استعمال کرنا ضروری ہے۔ لاپرواہی سے استعمال رازداری کے خطرات، سائبر خطرات اور ذاتی معلومات کے غلط استعمال کا باعث بن سکتا ہے۔

5- رازداری کی ترتیبات ڈیجیٹل پلیٹ فارم پر ذاتی معلومات کی حفاظت میں کس طرح مدد کرتی ہیں؟

جواب: رازداری کی ترتیبات صارفین کو یہ کنٹرول کرنے کی اجازت دیتی ہیں کہ ان کی معلومات کو کون دیکھ سکتا ہے، جیسے پوسٹس اور ذاتی تفصیلات۔ ان ترتیبات کو باقاعدگی سے اپ ڈیٹ کرنے سے ذاتی ڈیٹا کو غیر مجاز رسائی یا غلط استعمال سے بچانے میں مدد ملتی ہے۔

6- رازداری کے قوانین افراد اور تنظیموں کی حفاظت میں کس طرح مدد کرتے ہیں، اور ان ضوابط پر عمل کرنا کیوں ضروری ہے؟

جواب: حکومت کی طرف سے مقرر کردہ رازداری کے قوانین ذمہ دارانہ ڈیٹا ہینڈلنگ کو یقینی بنا کر ذاتی معلومات کی حفاظت کرتے ہیں۔ وہ یہ ریگولیٹ کرتے ہیں کہ کون سا ڈیٹا اکٹھا کیا جا سکتا ہے، اسے کیسے استعمال کیا جاتا ہے، اور کون اس تک رسائی حاصل کر سکتا ہے۔ ان قوانین پر عمل کرنا ذاتی ڈیٹا کے غلط استعمال کو روکتا ہے اور تنظیم میں اخلاقی ذمہ داری کو یقینی بناتا ہے۔

7- ساکھ کی تشخیص کیا ہے، اور آن لائن تحقیق کرتے وقت یہ کیوں ضروری ہے؟

جواب: اعتبار کی تشخیص آن لائن معلومات کی درستگی اور اعتماد کی تصدیق کا عمل ہے۔ غلط معلومات کو روکنا اور اس بات کو یقینی بنانا ضروری ہے کہ صارفین مستند ذرائع پر انحصار کریں۔ متعدد ذرائع کی جانچ کرنا، سنسنی خیز سرخیوں پر شک کرنا، اور .edu یا .gov ویب سائٹس کو ترجیح دینا کلیدی حکمت عملی ہیں۔

8- کمپیوٹنگ معاشرے کے مختلف پہلوؤں، جیسے اخلاقی، ماحولیاتی، قانونی، سماجی، اقتصادی اور ثقافتی اثرات کو کس طرح متاثر کرتی ہے؟

جواب: کمپیوٹنگ بہت سے شعبوں کو متاثر کرتی ہے:

اخلاقی اثر: کاپی رائٹ کی خلاف ورزی جیسے خدشات کو جنم دیتا ہے۔

ماحولیاتی اثرات: ای۔ فضلہ اور توانائی کی کھپت کا باعث بنتا ہے۔

قانونی اثر: رازداری کے قوانین اور دانشورانہ املاک کے حقوق شامل ہیں۔

سماجی اثر: مواصلات کو بہتر بناتا ہے لیکن رازداری کی خلاف ورزیوں کا سبب بن سکتا ہے۔

اقتصادی اثر: روزگار پیدا کرتا ہے لیکن روایتی کرداروں کی جگہ بھی لے لیتا ہے۔

ثقافتی اثرات: عالمی تجارت اور ڈیجیٹل موافقت کو متاثر کرتا ہے۔

خلاصہ

- محفوظ اور ذمہ دارانہ کمپیوٹر کے استعمال کا مطلب یہ ہے کہ یہ جاننا کہ ہماری ذاتی معلومات کی حفاظت کیسے کی جائے، ہم جو ہارڈ ویئر اور سافٹ ویئر استعمال کرتے ہیں اس کے بارے میں دانشمندانہ انتخاب کرنا، اور اس بات کو یقینی بنانا کہ ہمارا آن لائن برتاؤ قابل احترام اور اخلاقی ہو۔
- ذمہ دار کمپیوٹر کے استعمال کا مطلب ہے کمپیوٹر استعمال کرتے وقت اپنی اور دوسروں کی حفاظت کرنا۔
- ڈیجیٹل پلیٹ فارمز اور آلات کے محفوظ آپریشن کا مطلب ہے کہ ان کا اس طرح استعمال کریں جو آپ کو نقصان سے بچاتا ہے اور کسی بھی ناپسندیدہ مسائل سے بچتا ہے۔
- ڈیجیٹل پلیٹ فارمز کو محفوظ طریقے سے استعمال کرنے کا مطلب ہے آپ کی معلومات کی حفاظت کے لیے اضافی اقدامات کرنا اور اس بات کو یقینی بنانا کہ آپ کی آن لائن سرگرمیاں آپ کو یا دوسروں کو خطرے میں نہ ڈالیں۔

stepacademyofficial.com

- رازداری کی ترتیبات اور ڈیٹا کی حفاظت کے اقدامات ضروری ٹولز ہیں جو ڈیجیٹل پلیٹ فارم استعمال کرتے وقت آپ کی ذاتی معلومات کی حفاظت میں مدد کرتے ہیں۔
- رازداری کے قوانین حکومت کی طرف سے ہماری ذاتی معلومات کی حفاظت کے لیے مقرر کردہ اصول ہیں۔ یہ قوانین اس بات کو یقینی بناتے ہیں کہ کمپنیاں اور تنظیمیں ہمارے ڈیٹا کو ذمہ داری سے ہینڈل کریں۔
- ڈیٹا کے استعمال کے لیے اخلاقی رہنما خطوط میں اس بات کو یقینی بنانا شامل ہے کہ ڈیٹا کو اس مقصد کے لیے استعمال کیا جائے اور یہ کہ اسے فراہم کرنے والے کو فائدہ ہو۔
- دانشورانہ املاک کے حقوق اہم ہیں کیونکہ وہ افراد اور تنظیموں کی تخلیقات اور نظریات کی حفاظت کرتے ہیں۔
- کاپی رائٹ ایک قانونی حق ہے جو تخلیق کاروں کو ان کے اصل کاموں، جیسے موسیقی، کتابیں، فلمیں اور سافٹ ویئر پر کنٹرول دیتا ہے۔
- ٹریڈ مارک علامتیں، نام، یا نعرے ہیں جو کمپنیاں اپنی مصنوعات یا خدمات کو دوسروں سے ممتاز کرنے کے لیے استعمال کرتی ہیں۔
- پیٹنٹ نئی ایجادات یا عمل کی حفاظت کرتے ہیں، جس سے موجد کو ایک خاص مدت کے لیے ایجاد بنانے، استعمال کرنے یا فروخت کرنے کے خصوصی حقوق ملتے ہیں۔
- سافٹ ویئر پائریسی سافٹ ویئر کی غیر قانونی کاپی، تقسیم، یا استعمال ہے۔

حل مشقی سوالات

1۔ درست جواب کا انتخاب کریں:

(i) کمپیوٹر کو محفوظ طریقے سے اور ذمہ داری سے استعمال کرنا کیوں ضروری ہے؟

(الف) اس بات کو یقینی بنانے کے لیے کہ ہم انہیں زیادہ کثرت سے استعمال کر سکیں

(ب) ہماری ذاتی معلومات کی حفاظت کرنا اور ہارڈ ویئر اور سافٹ ویئر کے بارے میں دانشمندانہ انتخاب کرنا

(ج) کمپیوٹر کو تیزی سے چلانے کے لیے (د) سافٹ ویئر کی ادائیگی سے بچنے کے لیے

(ii) "کمپیوٹر کے ذمہ دار استعمال" میں کیا شامل ہے؟

(الف) سب سے مہنگے ہارڈ ویئر کا انتخاب کرنا (ب) اپنے پاس ورڈ دوستوں کے ساتھ بانٹنا

(ج) آپ جو کچھ آن لائن شیئر کرتے ہیں اس کے بارے میں محتاط رہنا اور اپنی اور دوسروں کی حفاظت کرنا

(د) سافٹ ویئر اپ ڈیٹس کو نظر انداز کرنا

(iii) ہارڈ ویئر اور سافٹ ویئر کی مطابقت کو یقینی بنانے کے لیے آپ کو کیا چیک کرنا چاہیے؟

(الف) ہارڈ ویئر کا رنگ

(ب) سافٹ ویئر پیکجز پر سسٹم کے تقاضے اور انہیں آپ کے کمپیوٹر کی تصریحات کے ساتھ ملائیں۔

(ج) ہارڈ ویئر کی قیمت (د) ہارڈ ویئر کا برانڈ

(iv) مضبوط، منفرد پاس ورڈ استعمال کرنا کیوں ضروری ہے؟

(الف) اپنے اکاؤنٹس کو ہیک کرنا آسان بنانے کے لیے

(ب) آپ کے پاس ورڈ کا اندازہ لگانے میں دوسروں کی مدد کرنے کے لیے

(ج) کسی کے لیے آپ کے پاس ورڈ کا اندازہ لگانا اور آپ کے اکاؤنٹس تک رسائی مشکل بنانا

(د) سافٹ ویئر اپ ڈیٹس انسٹال کرنے سے بچنے کے لیے

stepacademyofficial.com

https://stepacademyofficial.com/

(v) نامعلوم لنکس پر کلک کرنے یا ناقابل اعتماد ذرائع سے فائلیں ڈاؤن لوڈ کرنے سے بچنے کی ایک وجہ کیا ہے؟

(الف) ان میں مددگار سافٹ ویئر ہوسکتا ہے۔

(ب) ان میں میلویئر ہوسکتا ہے جو آپ کے آلے کو نقصان پہنچا سکتا ہے یا آپ کی معلومات چرا سکتا ہے۔

(ج) وہ عام طور پر سستے ہوتے ہیں۔

(د) وہ آپ کے آلے کو تیزی سے چلانے میں مدد کرتے ہیں۔

(vi) ٹو فیکٹر توثیق (2FA) کیا کرتا ہے؟

(الف) یہ آپ کے پاس ورڈ کا اندازہ لگانا آسان بناتا ہے۔

(ب) یہ توثیق کی دوسری شکل کی ضرورت کے ذریعے سکیورٹی کی ایک اضافی پرت کا اضافہ کرتا ہے۔

(ج) یہ پاس ورڈ کی ضرورت کو دور کرتا ہے۔

(د) یہ سافٹ ویئر اپ ڈیٹس کی ضرورت کو کم کرتا ہے۔

(vii) حساس لین دین کے لیے پبلک وائی فائی استعمال کرتے وقت آپ کو کیوں محتاط رہنا چاہیے؟

(الف) عوامی Wi-Fi عام پر تیز ہوتا ہے۔

(ب) عوامی Wi-Fi نیٹ ورک اکثر کم محفوظ ہوتے ہیں۔

(ج) پبلک وائی فائی مفت ہے۔

(د) پبلک وائی فائی ہمیشہ انکرپشن فراہم کرتا ہے۔

(viii) سوشل میڈیا کے ذمہ دارانہ استعمال کا ایک اہم پہلو کیا ہے؟

(الف) ذاتی معلومات کا اشتراک کرنا جیسے آپ کے گھر کا پتہ

(ب) رازداری کی ترتیبات پر غور کیے بغیر تصاویر پوسٹ کرنا

(ج) احترام کرنا اور حساس معلومات کو عوامی طور پر شیئر کرنے سے گریز کرنا

(د) رازداری کی ترتیبات کو نظر انداز کرنا

(ix) اگر آپ کو کسی نامعلوم ارسال کنندہ کی طرف سے ذاتی معلومات طلب کرنے والا ای میل موصول ہوتا ہے تو آپ کو کیا کرنا چاہیے؟

(الف) درخواست کردہ معلومات فراہم کریں۔

(ب) ای میل کو اپنے دوستوں کو بھیجیں۔

(ج) ای میل کو نظر انداز کریں یا حذف کریں۔

(د) ای میل کھولیں اور کسی بھی لنک پر کلک کریں۔

(x) اپنے اکاؤنٹ کی سرگرمی کا باقاعدگی سے جائزہ لینا کیوں ضروری ہے؟

(الف) اپنی رابطہ کی معلومات کو اپ ڈیٹ کرنے کے لیے

(ب) غیر معمولی سرگرمی کو تلاش کرنے اور یہ یقینی بنانے کے لیے آپ کے اکاؤنٹس محفوظ ہیں

(ج) اپنے دوستوں کی تعداد چیک کرنے کے لیے

(د) نئی ایپلیکیشنز ڈاؤن لوڈ کرنے کے لیے

(xi) ڈیجیٹل پلیٹ فارمز پر رازداری کی ترتیبات کا مقصد کیا ہے؟

(الف) اپنی پوسٹس کو پبلک کرنا

(ب) یہ کنٹرول کرنے کے لیے کہ کون آپ کی معلومات دیکھ سکتا ہے اور آپ کے ساتھ آن لائن تعامل کر سکتا ہے۔

(ج) پیروکاروں کی تعداد میں اضافہ کرنا

(د) خود بخود اپنی معلومات کا اشتراک کرنے کے لیے

(xii) ڈیٹا کی حفاظت کو یقینی بنانے کے لیے آپ کو کیا کرنا چاہیے؟

(الف) تمام اکاؤنٹس کے لیے ایک ہی پاس ورڈ استعمال کریں۔

(ب) اپنے پاس ورڈ دوستوں کے ساتھ شیئر کریں۔

(ج) مضبوط، منفرد پاس ورڈ استعمال کریں اور دو عنصری توثیق کو فعال کریں۔

(د) کسی بھی حفاظتی اقدامات کے استعمال سے گریز کریں۔

stepacademyofficial.com

(xiii) ڈیٹا کی اخلاقیات کا ایک اہم پہلو کیا ہے؟

(الف) ڈیٹا کو اپنی پسند کے مطابق استعمال کرنا
(ب) ڈیٹا کے استعمال میں شفافیت، رازداری کا احترام، اور جوابدہی
(ج) زیادہ سے زیادہ ڈیٹا اکٹھا کرنا
(د) ڈیٹا سکیورٹی کو نظرانداز کرنا

(xiv) سافٹ ویئر پائریسی کیا ہے؟

(الف) دوستوں کے ساتھ قانونی طور پر سافٹ ویئر کا اشتراک کرنا
(ب) سافٹ ویئر کی غیر قانونی کاپی، تقسیم، یا استعمال
(ج) کسی سرکاری ذریعہ سے سافٹ ویئر خریدنا
(د) سافٹ ویئر کو باقاعدگی سے اپ ڈیٹ کرنا

(xv) آپ آن لائن ملنے والی معلومات کی ساکھ کی تصدیق کیسے کر سکتے ہیں؟

(الف) ویب سائٹ پر اشتہارات کی تعداد چیک کر کے
(ب) متعدد معتبر ذرائع کا استعمال کرتے ہوئے اور مصنف کی اسناد کی جانچ کر کے
(ج) ویب سائٹ کے ڈیزائن کو دیکھ کر
(د) ویب سائٹ کی مقبولیت کے لحاظ سے

جوابات

(i) (ب)	(ii) (ج)	(iii) (ب)	(iv) (ج)	(v) (ب)	(vi) (ب)	(vii) (ب)	(viii) (ج)
(ix) (ج)	(x) (ب)	(xi) (ب)	(xii) (ج)	(xiii) (ب)	(xiv) (ب)	(xv) (ب)	

2۔ مختصر سوالات:

(i) کمپیوٹر کو محفوظ طریقے سے اور ذمہ داری سے استعمال کرنے کی کیا اہمیت ہے؟

جواب: کمپیوٹر کا محفوظ طریقے سے اور ذمہ داری کے ساتھ استعمال ڈیٹا کے نقصان کو روکتا ہے، رازداری کی حفاظت کرتا ہے، سائبر خطرات سے بچتا ہے، اور ٹیکنالوجی کے اخلاقی استعمال کو یقینی بناتا ہے۔

(ii) صحیح ہاڈویئر اور سافٹ ویئر کا انتخاب آپ کے کمپیوٹر کے استعمال کو کیسے متاثر کرتا ہے؟

جواب: ہم آہنگ ہارڈویئر اور سافٹ ویئر کا انتخاب کارکردگی کو بہتر بناتا ہے، کارکردگی کو بڑھاتا ہے، اور نظام کے ہموار کام کو یقینی بناتا ہے۔

(iii) اپنے کمپیوٹر پر اینٹی وائرس سافٹ ویئر استعمال کرنا کیوں ضروری ہے؟

جواب: اینٹی وائرس سافٹ ویئر ڈیٹا کی حفاظت کو یقینی بناتے ہوئے سسٹم کو وائرس، میلویئر اور دیگر بدنیتی پر مبنی خطرات سے بچاتا ہے۔

(iv) ہارڈویئر اور سافٹ ویئر کا انتخاب کرتے وقت اچھے طریقوں کی کچھ مثالیں کیا ہیں؟

جواب: مثالوں میں مطابقت کو یقینی بنانا، قابل اعتماد برانڈز سے خریداری، جائزے پڑھنا، اور نظام کی ضروریات کی جانچ کرنا شامل ہیں۔

(v) ہم آہنگ ہارڈویئر اور سافٹ ویئر کا انتخاب آپ کے کمپیوٹر کے تجربے کو کیسے بڑھا سکتا ہے؟

جواب: ہم آہنگ ہارڈویئر اور سافٹ ویئر غلطیوں کو کم کرتے ہیں، پیداواری صلاحیت میں اضافہ کرتے ہیں، اور ہموار کارکردگی کو یقینی بناتے ہیں۔

(vi) آپ کو اپنے اکاؤنٹس کے لیے مضبوط، منفرد پاس ورڈ کیوں بنانا چاہیے؟

جواب: مضبوط، منفرد پاس ورڈ ہیکنگ اور ذاتی معلومات تک غیر مجاز رسائی کے خطرے کو کم کرتے ہیں۔

(vii) باقاعدہ سافٹ ویئر اپ ڈیٹس کا مقصد کیا ہے؟

جواب: سافٹ ویئر کی فعالیت کو بہتر بنانے کے لیے باقاعدگی سے اپ ڈیٹس بگز کو ٹھیک کرتی ہیں، سیکورٹی کو بڑھاتی ہیں، اور نئی خصوصیات شامل کرتی ہیں۔

stepacademyofficial.com

https://stepacademyofficial.com/

(viii) آپ اپنے آپ کو نقصان دہ لنکس اور ڈاؤن لوڈ سے کیسے بچا سکتے ہیں؟

جواب: مشکوک لنکس پر کلک کرنے سے گریز کریں، صرف قابل اعتماد ذرائع سے فائلیں ڈاؤن لوڈ کریں، اور حفاظتی آلات استعمال کریں۔

(ix) ٹو فیکٹر توثیق (2FA) کیا ہے اور یہ کیوں مفید ہے؟

جواب: ٹو فیکٹر توثیق کے دوسرے مرحلے کی ضرورت کے ذریعہ ایک اضافی حفاظتی پرت کا اضافہ کرتا ہے، جیسے کوڈ، غیر مجاز رسائی کو مشکل بنا دیتا ہے۔

(x) حساس لین دین کے لیے پبلک وائی فائی کے استعمال سے گریز کرنا اچھا خیال کیوں ہے؟

جواب: پبلک وائی فائی غیر محفوظ ہے، اور ہیکرز حساس لین دین کے دوران ڈیٹا کو روک سکتے ہیں۔

(xi) آپ اس بات کی تصدیق کیسے کر سکتے ہیں کہ آیا کوئی ای میل یا پیغام اسکیم ہے؟

جواب: بھیجنے والے کے مشکوک پتے، گرائمر کی غلطیاں، فوری زبان، اور نامعلوم لنکس پر سے تصدیق ہو سکتی ہے۔

(xii) سوشل میڈیا پر جو کچھ آپ شیئر کرتے ہیں اس کے بارے میں محتاط رہنا کیوں ضروری ہے؟

جواب: بہت زیادہ شیئر کرنا رازداری کے مسائل، شناخت کی چوری، یا ذاتی معلومات کے غلط استعمال کا باعث بن سکتا ہے۔

(xiii) اگر آپ کو کسی نامعلوم ارسال کنندہ کی طرف سے ذاتی معلومات طلب کرنے والا ایک میل موصول ہوتا ہے تو آپ کو کیا کرنا چاہیے؟

جواب: جواب دینے سے گریز کریں، لنکس پر کلک نہ کریں، اور ای میل کو سپیم کے طور پر رپورٹ کریں۔

(xiv) آپ کی ذاتی معلومات سے متعلق رازداری کے قوانین کا کیا مقصد ہے؟

جواب: رازداری کے قوانین افراد کے ذاتی ڈیٹا کو غلط استعمال سے بچاتے ہیں اور رازداری کے حقوق کو یقینی بناتے ہیں۔

(xv) رازداری کے قوانین آپ کو آپ کے ڈیٹا تک غیر مجاز رسائی سے کیسے بچاتے ہیں؟

جواب: وہ ڈیٹا اکٹھا کرنے کو منظم کرتے ہیں، استعمال کے سخت قوانین کو نافذ کرتے ہیں، اور صارف کے ڈیٹا کی حفاظت کے لیے خلاف ورزیوں کو سزا دیتے ہیں۔

(xvi) کاپی رائٹ، ٹریڈ مارکس اور پیٹنٹ میں کیا فرق ہے؟

جواب: کاپی رائٹ کتابوں اور موسیقی جیسے اصل کاموں کی حفاظت کرتا ہے۔

ٹریڈ مارک برانڈ کے ناموں اور لوگو کی حفاظت کرتے ہیں۔

پیٹنٹ نئی ایجادات یا عمل کی حفاظت کرتے ہیں۔

(xvii) دانشورانہ املاک کے حقوق کا احترام کیوں ضروری ہے؟

جواب: دانشورانہ املاک کا احترام جدت طرازی کی حوصلہ افزائی کرتا ہے، تخلیق کاروں کی حمایت کرتا ہے، اور قانونی مسائل سے بچتا ہے۔

(xviii) سافٹ ویئر پائریسی کیا ہے، اور یہ کیوں نقصان دہ ہے؟

جواب: سافٹ ویئر کی پائریسی سافٹ ویئر کا غیر مجاز استعمال یا تقسیم ہے، جس کے قانونی نتائج اور ڈویلپرز کے لیے آمدنی کا نقصان ہوتا ہے۔

(xix) آن لائن تحقیق کرتے وقت آپ قابل اعتماد ذرائع کی شناخت کیسے کر سکتے ہیں؟

جواب: مصنف کی اسناد، ویب سائٹ ڈومین، اشاعت کی تاریخ، اور کراس تصدیق کی معلومات چیک کریں۔

(xx) آن لائن تحقیق کے دوران آپ کی رازداری کی حفاظت کا ایک طریقہ کیا ہے؟

جواب: محفوظ کنکشن استعمال کریں، ذاتی معلومات شیئر کرنے سے گریز کریں، اور براؤزر کی رازداری کی ترتیبات کو فعال کریں۔

stepacademyofficial.com

(xxi) کیا کچھ علامات ہیں جو آپ کو انٹرنیٹ کی لت میں مبتلا کر رہے ہیں؟

جواب: علامات میں آن لائن ضرورت سے زیادہ وقت گزارنا، ذمہ داریوں کو نظر انداز کرنا، آف لائن ہونے پر موڈ میں اتار چڑھاؤ، اور سماجی تعاملات سے دستبرداری شامل ہیں۔

3۔ تفصیلی سوالات

(i) آج کی ڈیجیٹل دنیا میں کمپیوٹر کے ذمہ دارانہ استعمال کی اہمیت پر تبادلہ خیال کریں۔ وضاحت کریں کہ کس طرح صحیح ہارڈ ویئر اور سافٹ ویئر کا انتخاب کمپیوٹر کے استعمال میں حفاظت، کارکردگی اور مطابقت کو متاثر کر سکتا ہے۔

جواب: جواب کے لیے دیکھیے سوال نمبر 1

(ii) ان اقدامات کی وضاحت کریں جو آپ کو ڈیجیٹل پلیٹ فارمز اور آلات کے محفوظ آپریشن کو یقینی بنانے کے لیے اٹھانے چاہئیں۔

جواب: جواب کے لیے دیکھیے سوال نمبر 2

(iii) ڈیٹا اخلاقیات کے تصور اور ذاتی اور حساس معلومات کو سنبھالنے میں اس کی اہمیت کی وضاحت کریں۔ شفافیت، رازداری کا احترام، اور جوابدہی کے اصولوں پر بحث کریں۔

جواب: جواب کے لیے دیکھیے سوال نمبر 4

(iv) ڈیجیٹل دور میں ذاتی معلومات کے تحفظ پر رازداری کے قوانین کے اثرات کا تجزیہ کریں۔ پاکستان میں پرسنل ڈیٹا پروٹیکشن بل جیسے قوانین صارف کے ڈیٹا کی حفاظت میں کس طرح مدد کرتے ہیں؟

جواب: جواب کے لیے دیکھیے سوال نمبر 4

(v) مختلف قسم کے دانشورانہ املاک کے حقوق پر تبادلہ خیال کریں، بشمول کاپی رائٹ، ٹریڈ مارکس، اور پیٹنٹ۔

جواب: جواب کے لیے دیکھیے سوال نمبر 5

(vi) انٹلیکچوئل پراپرٹی کے حقوق سے متعلق اخلاقی اور قانونی ذمہ داریوں کی وضاحت کریں۔ ان حقوق کی خلاف ورزی کے کیا نتائج ہیں، جیسے کہ سافٹ ویئر پائریسی کے ذریعے یا کاپی رائٹ شدہ مواد کا غیر مجاز استعمال؟

جواب: جواب کے لیے دیکھیے سوال نمبر 5

(vii) محفوظ اور معتبر آن لائن تحقیق کرنے کے لیے موثر تکنیکوں کا خاکہ پیش کریں۔ صارفین اپنی تحقیق کے دوران ذرائع کی وثوسنیتا کا اندازہ کیسے لگا سکتے ہیں اور رازداری کے خطرات سے کیسے بچ سکتے ہیں؟

جواب: جواب کے لیے دیکھیے سوال نمبر 6

(viii) انٹرنیٹ کی لت کے تصور اور افراد پر اس کے ممکنہ اثرات پر بحث کریں۔ نشے کی علامات کو پہچاننا، وقت کی حد مقرر کرنا، اور آف لائن سرگرمیاں تلاش کرنا متوازن انٹرنیٹ استعمال کو فروغ دینے میں کس طرح مدد کر سکتا ہے؟

جواب: جواب کے لیے دیکھیے سوال نمبر 7

stepacademyofficial.com
https://stepacademyofficial.com/