

سائبر تحفظ اور سلامتی کی بنیادی باتیں



سائبر تحفظ اور سلامتی کیا ہے؟

سائبر تحفظ اطلاعاتی و مواصلاتی ٹیکنالوجی کا محفوظ اور ذمہ دارانہ استعمال ہے۔ اس کا تعلق نہ صرف معلومات کے تحفظ اور محفوظ رکھنے تک محدود ہے بلکہ معلومات کے ساتھ ذمہ دار ہونے، آن لائن دوسرے لوگوں کا احترام کرنے، اور انٹرنیٹ آداب کی پابندی کرنے سے بھی ہے۔ اس میں نیٹ ورک، کمپیوٹر، پروگراموں اور ڈیٹا کو حملے، نقصان یا غیر مجاز رسائی سے بچانے کے لیے ڈیزائن کردہ ٹیکنالوجی پر عمل اور طریقہ کار شامل ہیں۔

سائبر ہراسانی سے واسطہ پڑنے پر درج ذیل کام کریں

جواب نہ دیں

اگر آپ کا سائبر ہراسانی سے واسطہ پڑ رہا ہے تو اسی طرح جواب دینے یا جوابی کارروائی سے بچیں۔ سائبر ہراسانی کا جواب ویسا ہی دینا یا جوابی کارروائی کرنا معاملہ کو مزید خراب کر سکتا ہے یا آپ کو پریشانی میں ڈال سکتا ہے۔

اسکرین شاٹ

اس چیز کا اسکرین شاٹ لیں جو آپ کے خیال میں سائبر ہراسانی ہو سکتی ہے اور اس کو محفوظ رکھیں۔

بلاک اور رپورٹ

ہراساں کرنے والے کے بارے میں تنظیمیں اور ذمہ داران کو رپورٹ کریں اور بلاک کر دیں۔ زیادہ تر آن لائن پلیٹ فارم میں یہ سہولت موجود ہے کہ اگر کوئی آپ کو پریشان کرتا ہے، تو آپ سوشل میڈیا پلیٹ فارم پر ہراساں کرنے والے کو بلاک کر کے اس سائٹ کے منتظم/ذمہ دار کو رپورٹ کریں۔

اس کے بارے میں کس سے بات کریں؟

سائبر ہراسانی آپ کو کئی طرح سے نقصان پہنچا سکتی ہے۔ یہ نہ سمجھیں کہ آپ اکیلے ہیں۔ اپنے والدین اور اساتذہ کو بتائیں کہ کیا ہو رہا ہے۔ اس بات کو خود تک محدود نہ رکھیں۔

پرائیویسی بنائے رکھیں

اپنی سوشل میڈیا پرائیویسی (رازداری) سیٹنگ کو محفوظ رکھیں اور کسی ایسے شخص سے رابطہ نہ کریں جسے آپ آف لائن نہیں جانتے۔ جب آپ اجنبی لوگوں سے عام طور پر بات نہیں کرتے ہیں، تو آن لائن کیوں کریں؟

مختار رہیں

سائبر دنیا کی تمام احتیاطی اور حفاظتی تدابیر سے باخبر رہیں۔

سائبر دنیا میں محفوظ رہیں



سنٹرل انسٹی ٹیوٹ آف ایجوکیشنل ٹیکنالوجی
نیشنل کونسل آف ایجوکیشنل ریسرچ اینڈ ٹریننگ
سری ار بند و مارگ، نئی دہلی-110016

ٹیلی فون: 011 26962580 | فیکس: 011 26864141
ای میل: jdciet.ncert@nic.in

سائبر ہراسانی

سائبر ہراسانی میں کسی کے بارے میں منفی، نقصان دہ، جھوٹی یا لغو معلومات اور مواد بھیجنا، پوسٹ کرنا یا شیئر کرنا شامل ہے۔ یہ ایک سنگین جرم ہے جو سائبر قانون کے تحت قابل سزا ہے۔

سائبر ہراسانی میں شامل ہے

- آپ کی پوسٹ یا آپ کے بارے میں نازیبا تبصرے
- آپ کے نام سے جعلی پروفائل بنا کر آپ کو بدنام کرنے کی کوشش کرنا
- آن لائن یا موبائل فون پر دھمکی آمیز یا گالی گلوں والے پیغامات بھیجنا
- آن لائن گروپ اور فورم سے خارج کیا جانا۔ آپ کو زبردستی باہر نکال دیا جانا
- آپ کی اجازت کے بغیر آن لائن تصاویر لگانا جو آپ کے لیے شرمندگی یا صدمے کا باعث ہو
- کسی سائٹ پر آپ کے بارے میں جھوٹی باتیں یا افواہیں پھیلانا
- آپ کے اکاؤنٹ کا پاس ورڈ چوری کرنا اور آپ کے اکاؤنٹ سے ناپسندیدہ/غیر مناسب پیغامات بھیجنا
- جارحانہ گفتگو یا مراسلت
- آپ کو بدنام کرنے کے لیے آپ کا جعلی آن لائن پروفائل بنانا



VIRUS



011-26864141
011-26962580
011-26864141



محفوظ سوشل نیٹ ورکنگ

- ذاتی معلومات جیسے عمر، پتہ، ٹیلی فون نمبر، اسکول کا نام وغیرہ ظاہر کرنے سے گریز کریں کیونکہ ان کا غلط استعمال ہو سکتا ہے۔
- سوشل نیٹ ورکنگ سائٹ پر اپنی پرائیویسی سیٹنگ کے تئیں محتاط رہیں۔
- والدین یا سرپرست کے علاوہ کبھی بھی اپنا پاس ورڈ کسی اور کو نہ بتائیں۔
- صرف اپنے جاننے والے لوگوں کے ساتھ ہی رابطہ اور تعاون کریں۔
- کوئی بھی ایسی پوسٹ شیئر نہ کریں جس سے دوسروں کے جذبات مجروح ہوتے ہوں۔
- سوشل نیٹ ورکنگ سائٹ پر تصاویر، ویڈیو اور کوئی دوسری حساس معلومات پوسٹ کرتے وقت ہمیشہ محتاط رہیں کیونکہ ان کی نقل (ڈیجیٹل فٹ پرنٹ) ہمیشہ آن لائن موجود رہتی ہیں۔
- نیٹ ورکنگ سائٹ پر اپنے دوستوں کی معلومات پوسٹ نہ کریں، یہ ان کے لیے خطرے کا سبب ہو سکتا ہے۔ گروپ فوٹو، جائے وقوع، عمر، اسکول کے نام وغیرہ پوسٹ نہ کر کے اپنے دوستوں کی رازداری کی حفاظت کریں۔
- نیٹ ورکنگ سائٹ پر اپنے منصوبوں اور سرگرمیوں کو عام کرنے سے گریز کریں۔
- کسی بھی سوشل نیٹ ورکنگ سائٹ پر اپنا جعلی پروفائل نہ بنائیں۔ اگر آپ کو شک ہے کہ آپ کے سوشل نیٹ ورکنگ اکاؤنٹ کی تفصیلات خطرے میں ہیں یا چوری ہو گئی ہیں، تو فوری طور پر نیٹ ورکنگ سائٹ کے منتظمین (Support team) کو اطلاع دیں۔
- سوشل میڈیا پر جو کچھ بھی آپ پڑھتے ہیں اس سے کسی قابل اعتماد ذریعہ سے تصدیق کیے بغیر کسی اور کو نہ بھیجیں۔
- سوشل نیٹ ورکنگ سائٹ پر لنک اور ایپلیکیشن کو کھولنے سے ممکنہ حد تک گریز کریں۔
- لاگ ان کرنے کے بعد اپنے اکاؤنٹ کو کبھی بھی ایسی غیر موجودگی میں کھلا نہ چھوڑیں، جب استعمال نہ کر رہے ہوں تو فوراً لاگ آؤٹ کر دیں۔

انٹرنیٹ تحفظ اور اخلاقیات

- دوسرے لوگوں کی پرائیویسی کا احترام کریں۔
- چیٹنگ، بلاگنگ اور ای میل کرتے وقت زبان کے استعمال سے متعلق مناسب پروٹوکول (آداب) پر عمل کریں۔
- کسی دوسرے کے ای میل اکاؤنٹس میں لاگ ان نہ کریں۔
- کاپی رائٹ والے مواد کو ڈاؤن لوڈ اور استعمال نہ کریں۔
- نقصان دہ سائٹ کا پتہ لگانے کے لیے خود کار براؤزر اپ ڈیٹ کو فعال رکھیں۔

محفوظ ای میل کے طریقے

- نامعلوم ارسال کنندہ کے ای میل کا جواب نہ دیں چاہے وہ حقیقی ای میل ہی کی طرح کیوں نہ لگ رہا ہو۔
- ذاتی معلومات جیسے نام، تاریخ پیدائش، اسکول کا نام، پتہ، والدین کے نام یا کوئی اور معلومات فراہم نہ کریں۔
- منافع بخش پیشکش اور عائدوں کے لالچ میں نہ پڑیں کیونکہ وہ نامعلوم ذرائع سے آرہی ہوں اور دھوکہ ہی ہوں۔ اس قسم کے میل کو نظر انداز / حذف کریں۔
- نامعلوم بھیجے والوں کے ایپلیکیشن کو نہ کھولیں اور نہ ہی لنک پر کلک کریں کیونکہ ان میں نقصان دہ فائلیں ہو سکتی ہیں جو آپ کے سسٹم کو خراب کر سکتی ہیں۔ صرف ایسے لنکس پر کلک کریں اور ان ہی ویب سائٹس سے ڈاؤن لوڈ کریں جن پر آپ بھروسہ کرتے ہیں۔
- دھوکہ دہی والی ویب سائٹ سے ہوشیار رہیں یہ تصدیق کرنے کے لیے URL چیک کریں کہ کیا ویب سائٹ محفوظ ہے۔
- آپ کو موصولہ اسپیم یا مشکوک ای میل دوسروں کو نہ بھیجیں۔



کمپیوٹر کا تحفظ اور سلامتی

- جب کمپیوٹر استعمال میں نہ ہو تو اسے لاگ آف کر دیں اور غیر موجودگی میں کھلا نہ چھوڑیں۔
- بجلی کا پلگ کمپیوٹر سے براہ راست نہ لگائیں، کیونکہ وہ الٹج زیادہ ہونے پر کمپیوٹر خراب ہو سکتا ہے۔ اس کے بجائے، کمپیوٹر اسٹینڈائزر کا استعمال کریں۔
- مسروقہ سافٹ ویئر انسٹال نہ کریں۔
- نامعلوم آلات کو اپنے کمپیوٹر سے کنکٹ نہ کریں کیونکہ ان میں وائرس ہو سکتے ہیں۔
- صرف تصدیق شدہ اوپن سورس یا لائسنس یافتہ سافٹ ویئر اور آپریٹنگ سسٹم استعمال کریں۔
- چیک کریں کہ ہر سسٹم میں اینٹی وائرس سافٹ ویئر باقاعدگی سے اپ ڈیٹ ہے۔
- ایک مضبوط فائر وال (حفاظتی دیوار) کا استعمال کریں۔
- مواد فلٹرینگ سافٹ ویئر کا استعمال کرتے ہوئے .bat, .cmd, .exe, .pif جیسے فائل ایکسٹینشن کو بلاک کر دیں۔
- مخصوص پروٹوکول ہدایات کے مطابق مضبوط پاس ورڈ بنائیں، اپنے پاس ورڈ کو وقفے وقفے سے تبدیل کریں، پرانے پاس ورڈ کو دوبارہ استعمال نہ کریں۔
- اس بات کو یقینی بنائیں کہ کمپیوٹر سسٹم اور لیپ میں اس کی مدد صرف وہی اہلکار کر رہے ہیں، جن کو مقرر کیا گیا ہے۔
- نیٹ ورک پر ذاتی آلات جیسے ذاتی یو۔ایس۔بی۔ (USB) یا ہارڈ ڈرائیو کے استعمال سے بچیں۔