سائبر دنیا میں محفوظ رہیں

اساتذہ کیا کریں اور کیا نہ کریں

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

ڈیولپمنٹ کمیٹی

چیئر پرسن

امریندر بہرا، پروفیسر اور جوائنٹ ڈائریکٹر، سنٹرل انسٹی ٹیوٹ آف ایجوکیشنل ٹیکنالوجی (سی آئی ای ٹی)، این سی ای آر ٹی، نئی دہلی

ممبر کوآرڈی نیٹر

ہنجل رتنا بائی، اسسٹنٹ پروفیسر، سینٹرل انسٹی ٹیوٹ آف ایجوکیشنل ٹیکنالوجی (سی آئی ای ٹی)، این سی ای آر ٹی، نئی دہلی

اراکین

ایم۔یو۔پائلی، پروفیسر آر آئی ای، این سی ای آر ٹی، میسور، کرناٹک

اندو کمار، ایسوسی ایٹ پروفیسر اور ہیڈ، ڈی آئی سی ٹی اینڈ ٹی ڈی، سی آئی ای ٹی، این سی ای آر ٹی، نئی دہلی

مامور علی، اسسٹنٹ پروفیسر، سی آئی ای ٹی، این سی ای آر ٹی، نئی دہلی

ریجاالکریم باربھوئیا، اسسٹنٹ پروفیسر، ڈی ای ایس ایم، این سی ای آر ٹی، نئی دہلی

رامنوجم میگنا تھن، ایسوسی ایٹ پروفیسر، ڈی ای ایل، این سی ای آر ٹی، نئی دہلی

ڈی۔وردا ایم۔نکالجے، ایسوسی ایٹ پروفیسر، ڈی ای ای، این سی ای آر ٹی، نئی دہلی

سربھی، اسسٹنٹ پروفیسر، سی آئی ای ٹی، این سی ای آر ٹی، نئی دہلی

آئی۔ایل۔نرسمہاراؤ، پروجیکٹ مینیجر II، سینٹر فار ڈیولپمنٹ آف ایڈوانسڈ کمپیوٹنگ (CDAC)، حیدر آباد، تلنگانہ

سجاتا مکھرجی، گلوبل ریسرچ اینڈ اے پی اے سی آؤٹ ریچ لیڈ، گوگل انڈیا پرائیویٹ لمیٹڈ حیدر آباد، تلنگانہ

ونیت کمار، بانی اور صدر، سائبر پیس فاؤنڈیشن، رانچی، جھارکھنڈ

چاندنی اگروال (نیشنل آئی سی ٹی ایوارڈ یافتہ)، سربراہ، شعبۂ کمپیوٹر سائنس، مہاراجہ اگرسین ماڈل اسکول، نئی دہلی

ونیتا گرگ، صدر، شعبہ کمپیوٹر سائنس، شہید راجپال ڈی اے وی پبلک اسکول، نئی دہلی

سائبر دنیا میں محفوظ رہیں

ٹیکنالوجی نے مقام اور قومیت کی رکاوٹوں کو توڑ کر ہمیں اس طرح باہم مربوط کر دیا ہے جس کا 20 سال پہلے تصور بھی نہیں کیا جا سکتا تھا۔ حالیہ برسوں میں ہماری تہذیب کی اہم ترین ترقی تکنیکی کامیابیوں کی مرہون منت ہے۔ تاہم، ہر چیز کا ایک دوسرا پہلو بھی ہوتا ہے۔ ٹیکنالوجی کی دنیا، خاص طور پر طلبا کے لیے خطرناک بھی ہو سکتی ہے۔ چند غلطیاں بچے کو حقیقی خطرے میں ڈال سکتی ہیں۔ 'انٹرنیٹ استعمال کرنے والے طلبا کے لیے' آن لائن تحفظ' کی تجویز پیش کی گئی ہے۔ آن لائن تحفظ صرف درج ذیل پابندیوں تک ہی محدود نہیں ہے...

- انٹرنیٹ کا محدود استعمال
- بہت زیادہ آن لائن پابندیاں
- شدید انٹرنیٹ مانیٹرنگ
- ویب سائٹس کو بلاک کرنا

اساتذہ اکثر اوقات اپنے طلبا کے 'تحفظ' کے لیے ان ہدایات کا استعمال کرتے ہیں۔ لیکن آن لائن تحفظ صرف ان ہدایات تک ہی محدود نہیں ہے۔

کسی نے ٹھیک کہا ہے، ''اگر آپ کسی شخص کو مچھلیاں مہیا کرا دیتے ہیں تو اسے صرف ایک دن کھانا کھلاتے ہیں۔ لیکن اگر اسے مچھلی پکڑنا سکھا دیتے ہیں تو اسے ساری زندگی کھانا کھلاتے ہیں۔''

اسی طرح، انٹرنیٹ سرفنگ کے دوران طلبا پر انٹرنیٹ کی پابندیاں عائد کرنے کے بجائے انھیں آن لائن محفوظ رہنے کے ساتھ ساتھ اچھی عادتوں پر عمل کرنا سکھایا جانا چاہیے۔

1

تکنیکی پہلو
کیا کریں اور کیا نہ کریں

1. انٹرنیٹ پر معلومات تلاش کرتے وقت، تلاش کے محفوظ متبادلات استعمال کریں۔ معلومات کو شیئر کرنے یا آگے بھیجنے سے پہلے حقائق کی جانچ کریں۔

2. آن لائن بینکنگ، خریداری یا آن لائن ادائیگی کرتے وقت، یہ دیکھیں کہ آیا ویب سائٹ کا یو آر ایل "https" سے شروع ہوتا ہے یا نہیں ("s" کا مطلب 'Safe' یعنی محفوظ' ہے)، اس کے علاوہ، سبز ایڈریس بار یا سیکیورٹی سرٹیفکیٹ دیکھیں (بند تالے کی شکل کے آئکن کے ذریعہ اس کی نشاندہی کی جاتی ہے) جو محفوظ کنکشن کو یقینی بناتا ہے۔ اس بات کو یقینی بنانے کے لیے کہ ویب ایڈریس پر موجود نام وہی ہے جو سرٹیفکیٹ میں موجود ہے، سرٹیفکیٹ پر ڈبل کلک کریں۔

3. مختلف آن لائن لین دین کے لیے ایک ہی پاس ورڈ کا استعمال نہ کریں۔

4. ہر اکاؤنٹ کے لیے ایک مضبوط اور منفرد پاس ورڈ کا استعمال کریں جو اعداد، بڑے چھوٹے حروف اور خصوصی حروف کا مجموعہ ہو۔

5. ذاتی اور کاروباری مقصد کے لیے الگ الگ ای میل اکاؤنٹس استعمال کریں۔ سوشل میڈیا سائٹس کے لیے کبھی بھی اپنا کاروباری ای میل ایڈریس استعمال نہ کریں۔

6. خریداری یا بینکنگ کے علاوہ انٹرنیٹ پر اور اپنے سوشل میڈیا پروفائل میں لاگ ان کرنے کے لیے بھی مفت اور غیر محفوظ وائی فائی استعمال کرنے سے گریز کریں۔

تکنیکی پہلو

7. جن اکاؤنٹ کو آپ استعمال نہیں کرتے ہیں انھیں حذف کر دیں۔

8. سافٹ ویئر قابل اعتماد ذرائع سے حاصل کریں۔ فائلوں کو کھولنے سے پہلے انھیں ہمیشہ اسکین کریں۔

9. ایڈریس بار میں اپنے بینک کی ویب سائٹ کا URL خود ٹائپ کر کے اس تک رسائی حاصل کریں۔ کبھی بھی کسی ای میل یا ٹیکسٹ میسیج سے اس تک رسائی حاصل نہ کریں۔

10. کسی بھی غیر متوقع یا غیر مطلوب ای میل کے لنک پر کلک نہ کریں اور نہ ہی منسلکات کو ڈاؤن لوڈ کریں خواہ وہ کسی معلوم ذریعے سے بھیجے ہوئے نظر آتے ہوں۔

11. تمام اہم فائلوں کا آف لائن/کلاؤڈ اسٹوریج پر باقاعدہ بیک اپ لیں۔

12. ویب سائٹ پر 'مجھے لاگ ان رکھیں' (Logged in) یا 'مجھے یاد رکھیں' (Remember me) کے متبادلات پر کلک نہ کریں اور تمام اکاؤنٹ لاگ آؤٹ کریں۔

13. کبھی بھی کوئی ذاتی معلومات جیسے نام، تاریخ پیدائش، پتہ وغیرہ کو اپنے پاس ورڈ کے طور پر استعمال نہ کریں۔

14. فون، ای میل یا ایس ایم ایس پر کبھی بھی ذاتی/بینک کی تفصیلات شیئر نہ کریں، خواہ فون کرنے والا/میسج بھیجنے والا معتبر کیوں نہ ہو۔

15. Pop-up بلوں اور مشکوک سروے پر کلک کرنے سے پہلے غور کریں، فائن پرنٹ پڑھیں، اور ٹاسک مینیجر سے ایسے تمام پاپ-اپ کو بند کر دیں۔

16. صرف تجسس کی بنیاد پر آپ غیر مناسب ویب سائٹ یا ایسی ویب سائٹ پر کبھی نہ جائیں جس سے آپ مکمل طور پر آگاہ نہ ہوں۔

17. اپنے کریڈٹ/ڈیبٹ کارڈ کی معلومات کو کسی بھی ویب سائٹس اور ویب براؤزر پر محفوظ نہ کریں۔

1

تکنیکی پہلو

18. مناسب وائی فائی نیٹ ورک سے جڑیں، جسے بصورت دیگر SSID کے نام سے جانا جاتا ہے۔
19. دو سطحی یا کثیر سطحی تصدیق کا استعمال کریں۔
20. جب ٹوکن، اسمارٹ کارڈ، پن یا صارف کی منتخب کردہ سیکیورٹی امیج جیسے دیگر متبادل دستیاب ہوں تو یوزر نیم اور پاس ورڈ استعمال نہ کریں۔
21. پاس ورڈ کی فہرست کو محفوظ جگہ پر رکھیں اور انہیں کم از کم تین ماہ میں ایک بار ضرور تبدیل کر دیں۔
22. اس بات کو یقینی بنائیں کہ کمپیوٹر میں تازہ ترین پیچ (Patch) ڈالے گئے ہیں۔ براؤزر، آپریٹنگ سسٹم اور اینٹی وائرس کو اپڈیٹ رکھیں۔
23. پہلے سے یہ رائے قائم نہ کریں کہ وائرس کا پتہ لگانے والا سافٹ ویئر ہمیشہ کمپیوٹر کے ساتھ کام کرتا ہے۔
24. کلاؤڈ اسٹوریج سسٹم میں خفیہ ڈیٹا شیئر/اپ لوڈ نہ کریں۔
25. تمام آن لائن لین دین کا ریکارڈ رکھیں اور اپنے بینک اکاؤنٹ کو باقاعدگی سے چیک کرتے رہیں۔
26. دوسرے آلات کی حفاظت کے لیے ڈومین نیم سسٹم (DNS) سروس شامل کریں۔

1

تکنیکی پہلو

27. جب آپ اپنے کمپیوٹر/ٹیبلیٹ/فون کو استعمال نہ کر رہے ہوں تو اپنی اسکرین کو لاک کر دیں اور اس کی سیٹنگ کو اس طرح تبدیل کر دیں کہ جب یہ سلیپ موڈ میں چلا جائے تو خود کار طور پر لاک ہو جائے۔

28. یہ کبھی نہ سمجھیں کہ آپ کے ڈیٹا کے رکھ رکھاؤ اور اس کی حفاظت کی ذمہ داری کسی اور کی ہے۔

29. ای میل کو احتیاط سے چیک کریں تا کہ اس بات کو یقینی بنایا جا سکے کہ سورس ہیڈر ایک درست ایڈریس سے ہے۔

30. کبھی بھی مضر ویب سائٹ کی لنک پر کلک کرنے کی غلطی نہ کریں کیوں کہ یہ آپ کے کمپیوٹر میں مال ویئر لوڈ کر سکتی ہے۔

31. اسپیم (ردی) ای میل کو ہمیشہ فوری طور پر حذف کریں اور کسی لنک پر بھول چوک کے نتیجے میں کلک کرنے سے بچنے کے لیے ٹریش باکس کو خالی کریں۔

32. ڈسکشن فورم/چیٹ روم پر دوسروں کے ساتھ بات چیت کرتے ہوئے، اس بات کو یقینی بنائیں کہ Caps Lock بٹن غیر فعال ہو کیوں کہ بات چیت کے دوران بڑے حروف میں ٹائپ کرنا اچھا نہیں سمجھا جاتا ہے۔

33. طلبا کے ذریعہ آلات کے استعمال، آلات پر خرچ ہونے والے وقت کی نگرانی کریں۔

34. ایسے پروفائل بنائیں جو صرف بچوں کے لیے ہوں، سرچ، ویڈیو سائٹس، وغیرہ پر دستیاب متبادلات استعمال کریں۔

35. طلبا صرف ان مواد/سائٹوں تک رسائی حاصل کریں جن کی انہیں اجازت ہے۔

36. بچوں کے ذریعے استعمال کیے جا رہے آلات پر براؤزنگ ہسٹری کا باقاعدگی سے جائزہ لیں۔

2

اخلاقی پہلو
کیا کریں اور کیا نہ کریں

1. دوسروں کی معلومات حاصل کرنے یا اس میں ترمیم کرنے کے لیے جان بوجھ کر کمپیوٹر کا استعمال نہ کریں۔ اس میں پاس ورڈ کی معلومات، فائلیں وغیرہ شامل ہو سکتی ہیں۔
2. سرقہ نہ کریں یعنی انٹرنیٹ سے معلومات (کتاب، موسیقی، ویڈیو، سافٹ ویئر وغیرہ) کی نقل نہ کریں کیونکہ یہ بے ایمانی ہے اور غیر قانونی بھی ہے۔ آپ کاپی رائٹ قوانین کی خلاف ورزی کے مرتکب ہو سکتے ہیں۔
3. اگر آپ مواد استعمال کرنا چاہتے ہیں تو اصل تخلیق کار سے اجازت حاصل کریں۔ وسائل کے اصل مالک کو ہمیشہ کریڈٹ اور انتساب فراہم کریں۔
4. لوگوں سے آن لائن بات چیت کرتے ہوئے کبھی بھی غلط شناخت فراہم نہ کریں۔
5. دوسروں کے تخلیقی کام سے نفع نہ کمائیں۔
6. حوالہ دے کر 10 % تک مواد کا استعمال کیا جا سکتا ہے۔ جہاں بھی ممکن ہو وضاحت کریں۔

3

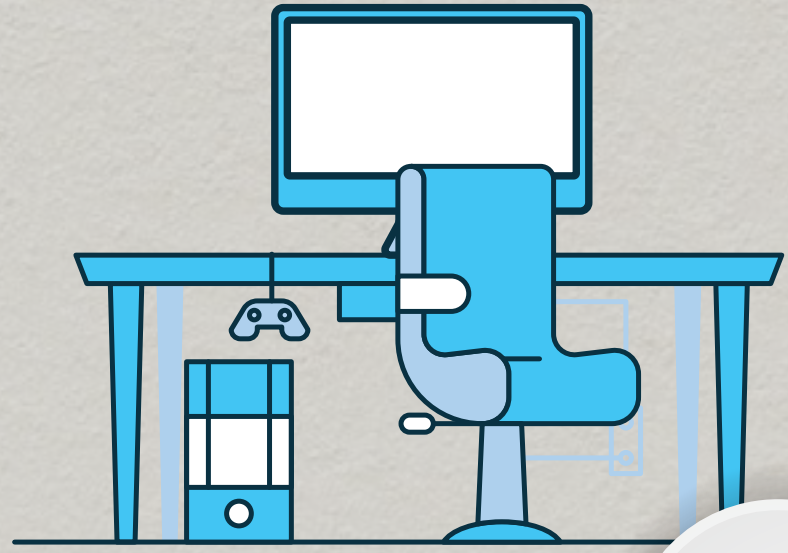
سماجی پہلو

1. ذاتی معلومات کو عام طور پر سوشل میڈیا سائٹ اور انٹرنیٹ پر شیئر کرنے سے گریز کریں۔
2. غیر مہذب، دھمکی آمیز یا توہین آمیز زبان استعمال کر کے سائبر ہراسانی کے مرتکب نہ ہوں۔
3. سائبر ہراسانی کرنے والوں کے ساتھ کوئی بات چیت یا بحث نہ کریں کیوں کہ اس کی وجہ سے خراب رویے کی حوصلہ افزائی ہو سکتی ہے۔
4. ای میل یا فوری پیغام رسانی کے ذریعے سائبر ہراسانی کرنے والوں سے بچنے کے لیے بِلٹ اِن فلٹر استعمال کریں۔
5. ان افراد سے کبھی بھی اکیلے نہ ملیں جن سے آپ کی صرف آن لائن شناسائی ہے۔
6. آن لائن کوئی ایسا کام نہ کریں جسے دوسروں کی موجودگی میں نہیں کیا جا سکتا۔
7. طلبا کے رویوں میں ہونے والی تبدیلیوں یا رویوں میں آنے والے فرق کی نگرانی کریں۔

4

قانونی پہلو
کیا کریں اور کیا نہ کریں

1. سائبر ہراسانی کی اطلاع متعلقہ حکام کو دیں۔ مزید کارروائی کے لیے سائبر ہراسانی کے مرتکب شخص سے موصول ہونے والے ہر تبصرے کا ریکارڈ رکھیں۔
2. کبھی بھی اُن ای میل پر بھروسہ نہ کریں جو لاٹری کے ذریعے انعامی رقم کی پیشکش کرتے ہیں جن میں آپ شریک نہیں ہیں۔ اسی طرح ان کاموں کے لیے ادائیگی نہ کریں جن کی درخواست آپ نے باضابطہ چینل کے ذریعے نہیں کی ہے۔
3. کسی سائٹ پر صرف اس لیے بھروسہ نہ کریں کہ وہ محفوظ ہونے کا دعوا کرتی ہے۔ یہ 'فشنگ سائٹ' (دھوکہ دہی میں ملوث) ہوسکتی ہے۔
4. ای میل اسپوفنگ (جعل سازی) سے بچیں۔
5. آن لائن خریداری کو فروغ دینے والے جعلی اشتہارات سے ہوشیار رہیں۔
6. غیر مجاز افراد/ڈیلروں سے کوئی بھی ڈیوائس نہ خریدیں۔
7. کسی بھی فرد کے ای میل کو کبھی نہ پڑھیں خواہ آپ کو اس کا پاس ورڈ کیوں نہ معلوم ہو۔



4

قانونی پہلو

کیا کریں اور کیا نہ کریں

8. کمپیوٹر سورس ریکارڈ کے ساتھ کبھی چھیڑ چھاڑ نہ کریں۔
9. فرد/تنظیم کی اجازت کے بغیر جمع کردہ ڈیٹا کو کبھی بھی شیئر یا تبدیل نہ کریں۔
10. کسی شخص کی رضامندی کے بغیر اس کی تصویر (تصویریں) نہ لیں، ان کی دوبارہ تخلیق یا ترسیل نہ کریں۔
11. کبھی بھی فحش مواد کو الیکٹرانک شکل میں شائع یا منتقل نہ کریں۔
12. بچوں کے ساتھ زیادتی پر مبنی کسی بھی الیکٹرانک مواد کی اطلاع متعلقہ حکام کو دیں۔
13. کوئی دھمکی بھرا، غیر مہذب یا ہتک آمیز ای میل نہ بھیجیں۔
14. اسکول سے تعلق رکھنے والے کمپیوٹر ہارڈ ویئر کو نہ چھپائیں۔
15. کبھی بھی کسی کاپی رائٹ مواد کی خلاف ورزی نہ کریں۔

سائبر قوانین

سیکشن	جرم	جرمانہ / سزا
67A	جنسی عمل پر مشتمل تصاویر شائع کرنا	سات سال تک قید یا/اور 1,000,000 روپے تک جرمانہ
67B	چائلڈ پورن شائع کرنا یا بچوں کے ساتھ آن لائن زیادتی کرنا	پہلی سزا پر 5 سال تک قید اور ایک سزا پر 1,000,000 روپے تک جرمانہ دوسری سزا پر 7 سال تک قید یا/اور 1,000,000 روپے تک جرمانہ
67C	ریکارڈ برقرار رکھنے میں ناکامی	3 سال تک قید یا/اور 2,00,000 روپے تک جرمانہ
68	احکامات کی تعمیل میں ناکامی/انکار	7 سال تک قید اور ممکنہ جرمانہ
69	ڈیٹا کو ڈی کرپٹ (رمز کشائی) کرنے میں ناکامی/انکار	3 سال تک قید یا/اور 100000 روپے تک جرمانہ
70	ایک محفوظ نظام تک رسائی حاصل کرنا یا رسائی حاصل کرنے کی کوشش کرنا	10 سال تک قید یا/اور جرمانہ
71	غلط بیانی	تین سال تک قید یا/اور 100000 روپے تک جرمانہ

CYBER SECURITY
MAJOR THREATS
PROTECTING
SAFE PRACTICE
Cyber Crime
committed for
Money
Curiosity
Revenge
Attention
Fun
Information & Devices
from
Modification
Destruction
Unauthorised Access
Disruption
Disclosure
Use/Misuse
Theft
Share
Changed
should be
do not
Securely
save
Password
Strong
should be
Firewall
use
Password
protect
use
Software
update
Desktop/ Laptop
backup
Data
no to
use & update
Pirated Software
use current/ updated
Antivirus
Operating System
regular/ automatic
Scan
Social Media
avoid
do not share
Strangers
use
ensure
Personal Informtion
Privacy Options
Security Options
User to be Old Enough
Cyber Laws
in
legal
for
WiFi
secure
E-mail Tracer
use
Latest Browser
use
Content Filtering
use
Internet
avoid
Friendship
in using
update
Browser Pluggins
Unknown People Online
avoid
Meeting in Person
Untrusted Website
never visit
do not open
avoid
E-mail Attachments
from
Unknown Persons
Referral Links
instead
Type the URL
Threats
any
check
URL
beware of
clean
Spy Camera
do not
Be Scared
save
Chat Screen
approach
Cyber Police
inform
Parents
Fake Account
Identity Theft
include
Morphing
E-Mail Bombing
Website Defacement
Hoax
means
Spam
Piracy
Malware
Hacking
Scam
Phishing
Copyright Violation
Spyware
Virus
Scareware
Ransomware
Worms
Trojans
Adware
include
obtaining
Sensitive Information
Before Discarding
format
Mobile Devices
download app from
Authorised Store
do not accept
Call from Weired Number
and do not
Call back
record
switch on
Bluetooth
only
When Needed
access only
Authorised WiFi
use
Auto Lock
IMEI Number
browser's cookies and cache
False Accusations
including
Slander
Libel
Defamation
Cyber Stalking
is
Repeated Harassment
Pornography
Websites
IM
through
E-mails
Online Groups
Phone
Insults
Lies
Rumors
Teasing
Threats
Name Calling
Threats
Cyber Bullying
Sexual Activities
Grooming
Harassments
Online Predators
uses
Social Engineering
Websites Spoofing
E-mail Spoofing
through
Click jacking
Tab Napping
Phone Call
Instant Messaging
like
Password
User Name
Credit Card Details
CC:BY:SA-M.U.Paily

www.ictcurriculum.gov.in

درسیات برائے تعلیم میں اطلاعاتی و مواصلاتی ٹیکنالوجی (آئی سی ٹی)

सत्यमेव जयते

Department of School Education & Literacy
Ministry of Human Resource Development
Government of India

تعلیم میں آئی سی ٹی کے لیے نمونہ جاتی درسیات ڈیجیٹل انڈیا پروگرام کے اہداف کو حاصل کرنے کا ایک اہم ذریعہ ہے۔ یہ درسیات اساتذہ اور طلبا کے لیے تیار کی گئی ہے تاکہ تدریس و آموزش کے فروغ اور معلومات کے ساتھ تنقیدی طور پر تعامل کرنے کے لیے آئی سی ٹی کے استعمال کی صلاحیتیں پیدا کی جاسکیں۔

درسیات کو چھ حصوں میں ترتیب دیا گیا ہے:

विद्यया ऽमृतमश्नुते
एन सी ई आर टी
NCERT

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

مزید تفصیلات معلوم کرنے کے لیے دیکھیں:

www.ncert.nic.in
www.ciet.nic.in
www.ictcurriculum.gov.in
www.infosecawareness.in
www.cyberswachhtakendra.gov.in