سائبر تحفظ اور سلامتی

اسکولوں کے لیے رہنما اصول

سائبر دنیا میں محفوظ رہیں...

ڈیولپمنٹ کمیٹی

چیئر پرسن

امریندر بہرا، پروفیسر اور جوائنٹ ڈائریکٹر، سی آئی ای ٹی، این سی ای آر ٹی، نئی دہلی

ممبر کوآرڈی نیٹر

اینجل رتنابائی، اسسٹنٹ پروفیسر، سی آئی ای ٹی، این سی ای آر ٹی، نئی دہلی

مترجمین

خورشید اکرم، سابق ڈپٹی ڈائریکٹر، آل انڈیا ریڈیو، نئی دہلی

راغب اختر، ایڈیٹر، بازگشت، نئی دہلی

ملک اشتر، سب ایڈیٹر (اردو)، دوردرشن، نئی دہلی

اردو کوآرڈی نیٹر

محمد فاروق انصاری، پروفیسر اور ہیڈ، ڈی ای ایل، این سی ای آر ٹی، نئی دہلی

رضوان الحق، اسسٹنٹ پروفیسر، سی آئی ای ٹی، این سی ای آر ٹی، نئی دہلی

تکنیکی ٹیم

شہناز بانو، اکیڈمک کنسلٹنٹ، سی آئی ای ٹی، این سی ای آر ٹی، نئی دہلی

ہمانشی بھاٹی، اکیڈمک کنسلٹنٹ، سی آئی ای ٹی، این سی ای آر ٹی، نئی دہلی

سائبر تحفظ سے مراد اطلاعاتی اور مواصلاتی ٹیکنالوجی کا محفوظ اور ذمہ دارانہ استعمال ہے۔اس کا تعلق صرف معلومات کو محفوظ رکھنے تک ہی محدود نہیں ہے، بلکہ اس معلومات کے تئیں ذمہ دار ہونے، آن لائن موجود دیگر افراد کا احترام کرنے اور انٹرنیٹ کے آداب (Netiquette) پر عمل کرنے سے بھی ہے۔

اطلاعاتی بنیادی ڈھانچہ اور انٹرنیٹ جیسے جیسے وسیع اور پیچیدہ ہوتا گیا ہے۔سسٹم کو فعال بنائے رکھنا اور حفاظتی امور کے معاملے میں متنبہ رہنا بھی خاصا اہم ہو گیا ہے۔اگرچہ حالیہ برسوں میں سسٹم ایڈمنسٹریشن کے کام آسان ہو گئے ہیں پھر بھی اسکولوں کے منتظمین کو سسٹم اور نیٹ ورک سیکورٹی کے بارے میں مزید اپ ڈیٹ رکھنے کی ضرورت ہے۔ حالیہ برسوں میں تمام سسٹم انٹرنیٹ کے رابطے میں آچکے ہیں؛ اس لیے ان کو سائبر حملوں سے محفوظ رکھنے میں ان کے حفاظتی سروکار مزید بڑھ گئے ہیں۔

انٹرنیٹ پر تحفظ کو فروغ دینے میں اسکول کلیدی کردار ادا کرتے ہیں۔اسکول بنیادی طور پر سسٹم/کمپیوٹر/نیٹ ورک آلات کو محفوظ اور فعال رکھنے کے لیے ذمہ دار ہیں۔معلومات کو محفوظ رکھنا اسی طرح ضروری ہے جیسے ہم کسی تنظیم میں سسٹم اور نیٹ ورک ڈیوائس کو رکھتے ہیں۔

فہرست

1 خطرے کی زد میں آنے کے اندیشے کی نشاندہی کریں اور خطرے کا اندازہ لگائیں

2 تحفظ اور خطرے کی نشاندہی کے طریقوں کو فروغ دیں

3 حساس ڈیٹا کی حفاظت کریں

4 سائبر تحفظ کے واقعات پر کاروائی کریں اور بازیافت کے لیے قدم اٹھائیں

5 متعلقہ لوگوں کو معلومات فراہم کریں

خطرے کی زد میں آنے کے اندیشے کی شناخت کریں اور خطرے کا اندازہ لگائیں

1

- سسٹم (مشین) کا دھیما اور سست رویہ
- کام کے دوران بلاوجہ سسٹم کی اسکرین کا غائب ہو جانا
- غیر متوقع پوپ اپ (pop ups) یا خلافِ معمول error پیغامات
- متوقع مدت سے قبل سسٹم کی بیٹری کا ختم ہو جانا
- بلو اسکرین آف ڈیتھ (BSOD) کا ظاہر ہونا
- بدنام زمانہ BSOD (بلو اسکرین آف ڈیتھ) کا ظاہر ہونا
- پروگرام/سسٹم کا اچانک بند ہونا
- اپ ڈیٹ کو ڈاؤن لوڈ نہ کر پانا
- بلا مقصد نئے براؤزر ہوم پیج، نئے ٹول بار/یا غیر ضروری ویب سائٹ پر چلے جانا
- آپ کے ای میل آئی ڈی سے آپ کے دوستوں کو عجیب و غریب پیغامات بھیجا جانا
- ڈیسک ٹاپ پر نئے اور غیر مانوس آئی کَن (icons) کا ظاہر ہونا
- خلافِ معمول پیغامات یا پروگراموں کا ظاہر ہونا جو خود بخود شروع ہو جاتے ہیں
- ٹاسک مینیجر میں غیر مانوس پروگرام کا متحرک ہونا

2

تحفظ اور خطرے کی نشاندھی کے طریقوں کو فروغ دیں

- ایک مضبوط فائروال کا استعمال کریں۔
- طلبا اور اساتذہ مضبوط پاس ورڈ بنائیں۔
- مضبوط پاس ورڈ سے متعلق ہدایات کے مطابق پاس ورڈ بنانے کی عادت کو فروغ دیں۔ پاس ورڈ بار بار تبدیل کریں، پرانے پاس ورڈ کے دوبارہ استعمال سے گریز کریں۔
- صرف تصدیق شدہ اوپن سورس یا لائسنس یافتہ سافٹ ویئر اور آپریٹنگ سسٹم استعمال کریں۔
- اس بات کو یقینی بنائیں کہ صرف مجاز اہلکاروں کو ہی کمپیوٹر سسٹم اور لیب تک رسائی حاصل ہو۔
- نیٹ ورک پر ذاتی USB یا ہارڈ ڈرائیو جیسے آلات کے استعمال سے بچنے کی تلقین کریں۔
- خود کار سافٹ ویئر اور آپریٹنگ سسٹم اپ ڈیٹ کے لیے اپنے کمپیوٹر کی سیٹنگ کو تبدیل کریں۔
- اس بات کی جانچ کریں کہ ہر سسٹم میں اینٹی وائرس سافٹ ویئر کو باقاعدگی سے اپ ڈیٹ کیا جاتا ہے۔
- مواد کو فلٹر کرنے والے سافٹ ویئر کا استعمال کر کے .bat,.cmd,.exe,.pif جیسے فائل ایکسٹینشن کو بلاک کرنے پر غور کریں۔

تحفظ اور خطرے کی نشاندھی کے طریقوں کو فروغ دیں

2

- فری ویئر اور شیئر ویئر (freeware and shareware) کو سسٹم پر انسٹال کرنے سے پہلے لائسنس کے معاہدے کو پڑھیں کہ آیا ان میں ایڈ ویئر اور اسپائی ویئر (adware and spyware) موجود نہیں ہیں۔
- انٹرنیٹ کے ذریعے دفتر یا اسکول لیب تک ریموٹ رسائی کے لیے SSL یا VPN جیسی رمز نگاری (encryption) کا استعمال کریں۔
- اس بات کو یقینی بنائیں کہ تھرڈ پارٹی وینڈر (جس کا اسکول کے ساتھ معاہدہ ہے) سخت حفاظتی تدابیر پر عمل کرتے ہوں۔
- اپنے اسکول کے نیٹ ورک تحفظ کی نگرانی کے لیے کسی قابل اعتماد/تصدیق شدہ تھرڈ پارٹی وینڈر کے ساتھ معاہدہ کرنے پر غور کریں۔
- طلبا، اساتذہ اور منتظمین کے لاگ اِن کے لیے دو سطحی یا کثیر سطحی تصدیق کو ضروری بنائیں۔
- اپنے Wi-Fi کنکشن کو مضبوط پاس ورڈ، WEP انکرپشن وغیرہ کی مدد سے تحفظ فراہم کریں۔
- نیٹ ورک ٹریفک کو اینکرپٹ کریں۔
- پہلے سے طے شدہ ایڈمنسٹریٹر پاس ورڈ کو تبدیل کریں۔ اگر وائرلیس نیٹ ورک کے پاس پہلے سے طے شدہ پاس ورڈ نہیں ہے تو نیا پاس ورڈ بنائیں اور اسے نیٹ ورک کی حفاظت کے لیے استعمال کریں۔
- کمپیوٹر پر فائل شیئرنگ کو غیر فعال کر دیں۔
- زیادہ دیر استعمال نہ ہونے کی صورت میں نیٹ ورک کو بند کر دیں۔
- "restricted mood"، "safesearch"، "supervised users" اور اسی طرح کے دیگر فلٹر اور مانیٹرنگ سسٹم استعمال کریں، تاکہ کوئی بچہ اسکول کے آئی ٹی سسٹم کے ذریعے نقصان دہ مواد تک رسائی حاصل نہ کر سکے اور کسی بھی تشویشناک بات کا فوراً پتہ لگایا جا سکے۔

3

حساس ڈیٹا کی حفاظت کریں

- اسٹوریج (استعمال شدہ/غیر استعمال شدہ) حساس معلومات تک رسائی اور تحفظ کا تعین کر کے اطلاعات کے تحفظ اور رسائی محدود کرنے کے پروگراموں اور پالیسیوں کو تیار اور نافذ کریں۔
- اہم معلومات کو کبھی بھی سسٹم کی سی (C) ڈرائیو میں محفوظ نہ کریں۔
- اہم ڈیٹا (رابطہ نمبر، ای میل آئی ڈی، آدھار نمبر وغیرہ) کا آف سائٹ لوکیشن پر بیک اپ تیار کریں۔
- سیکیورٹی کی خلاف ورزی کی اطلاع دینے والے شخص کی شناخت کے تحفظ کے لیے محفوظ رپورٹنگ کے رہنما خطوط اور اسکلیشن کے طور طریقے نافذ کریں۔

4

سائبر تحفظ کے واقعات پر کاروائی کریں اور بازیافت کے لیے قدم اٹھائیں

- **ابتدائی اندازۂ قدر:** مناسب کاروائی کو یقینی بنانے کے لیے ضروری ہے کہ کارروائی کرنے والی ٹیم اس بات کی نشاندہی کرے کہ:
  - واقعہ کیسے پیش آیا؟
  - کون سے IT اور/یا OT سسٹم متاثر ہوئے اور کیسے؟
  - کمرشیل/یا آپریشنل ڈیٹا کس حد تک متاثر ہوا؟
  - IT اور OT میں کس حد تک خطرہ باقی ہے؟
- **سسٹم اور ڈیٹا کی بازیافت کریں:** سائبر واقعہ کے ابتدائی اندازۂ قدر کے بعد، آئی ٹی اور او ٹی سسٹم اور ڈیٹا کو صاف کیا جانا چاہیے، جتنا ممکن ہو سکے ڈیٹا کی بازیافت اور بحالی کی جانی چاہیے تا کہ سسٹم سے خطرات کو ہٹا کر اور سافٹ ویئر کو رجال کر کے اسے کام کرنے کی حالت میں دوبارہ واپس لایا جا سکے۔
- **واقعہ کی تحقیقات کریں:** سائبر واقعے کی وجوہات اور نتائج کو سمجھنے کے لیے، اگر مناسب ہو تو کسی بیرونی ماہر یا کمپنی کے ذریعے تحقیقات کی جانی چاہیے۔ تحقیقات سے حاصل ہونے والی معلومات واقعہ کے دوبارہ رونما ہونے کے اندیشے کو ختم کرے گی۔
- **واقعہ کی تکرار نہ ہونے دیں:** مذکورہ تحقیقات کے نتائج کو دیکھتے ہوئے، اصلاح کے لیے کمپنی کے طریقۂ کار کے مطابق، تکنیکی اور/یا طریقۂ کار کے تحفظ کی تدابیر میں کسی بھی قسم کی کمی کو دور کیا جانا چاہیے۔

5

متعلقہ لوگوں کو معلومات فراہم کریں

- اسکولوں کے لیے 'کیا کریں اور کیا نہ کریں' عنوان کے تحت سائبر تحفظ کے قوانین مرتب کریں۔
- اسکول کے منتظمین کو ایسے جدید ترین ٹول کے بارے میں بتائیں جو ایسی ویب سائٹ کی نگرانی کے لیے استعمال کیے جاسکتے ہیں جنھیں طلبا/اساتذہ دیکھتے ہیں۔
- سائبر قوانین کے بارے میں متعلقہ لوگوں کی رہنمائی کریں (http://cyberlawsindia.net/)
- سائبر اسپیس میں خطرات اور ان سے بچاؤ کے اقدامات کے بارے میں بیداری کی سطح کو بڑھانے کے لیے سائبر اتحفظ سے وابستہ پیشہ ور افراد سے مشورہ کریں۔
- سائبر تحفظ اور سلامتی کے اہم اجزا پر طلبا اور اساتذہ کے لیے نصاب/اسباق/سرگرمیاں متعارف کرائیں۔
- ڈیجیٹل معلومات اور ٹیکنالوجی کے محفوظ، قانونی اور اخلاقی استعمال کی ترغیب دیں اور ضابطے بنائیں۔
- ٹیکنالوجی اور معلومات کے استعمال سے متعلق ذمہ دارانہ سماجی تعاملات کو فروغ دیں اور ضابطے بنائیں۔
- محفوظ انٹرنیٹ ڈے (5 فروری) منائیں اور سائبر کلبوں کے ذریعے آگاہی پیدا کرنے کے لیے سرگرمیاں انجام دیں۔
- کسی معروف سائبر سیکیورٹی فرم/تنظیم کے ساتھ رابطہ قائم کریں۔
- سائبر اسپیس میں اسکول کو محفوظ رکھنے کے لیے رہنما خطوط، پالیسیوں اور طریقۂ کار پر عمل کریں۔

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

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

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