کمپیوٹراستعمال کرنے والوں کے لئے ماہانہ سکیورٹی تعلیم کا نیوز لیٹر

OUCH!

اس شمارے میں شامل ہے:

- پس منظر
- خطرات
- بچوں کی تربیت

بچوں کو سائبر تحفظ کی تربیت دینا

پس منظر:

آج کے دور میں بچے جتنے طریقوں سے آن لائن ہوسکتے ہیں اور دوسروں سے بات کرسکتے ہیں وہ بہت ہی حیرت انگیز ہیں۔ نئی سوشل میڈیا سروسز بہت تیزی سے پھیل رہی ہیں اور ایسی ایپلیکیشنز اور گیمز کی تعداد بڑھتی جارہی ہے جو انٹرنیٹ سے منسلک ہونے کی صلاحیت رکھتی ہیں۔ اس کے علاوہ اسکولز، گوگل ڈرائیو جیسی سروسز کی طرف منتقل ہورہے ہیں جو آپ کو کام کا کچھ حصہ یا سارا کام آن لائن مکمل کرنے اور اسے جمع کرنے کی صلاحیت فراہم کرتی ہیں۔ آج کل بچے حقیقتاً آن لائن دنیا سے منسلک ہوتے ہوئے بڑے ہورہے ہیں- اس چیز کے جہاں فوائد ہیں وہاں کچھ خطرات بھی شامل ہیں۔ اس نیوز لیٹر میں ہم بچّوں کو لاحق تین خطرات پر روشنی ڈالیں گے اور اُن سے حفاظت کے طریقے بھی بتائیں گے۔

مہمان ایڈیٹر

باب رُوڈیس ،ویرائیزن میں سکیورٹی ڈیٹا سائنٹسٹ ہیں۔ وہ 2015ء ڈیٹا بریچ انویسٹیگیشن رپورٹ کے مصنّف اور چار بہت ہی زبردست بچوں کے والد ہیں۔ باب نے کئی فارچون 100 کمپنیوں میں سکیورٹی سے آگاہی کے مؤثر پروگرامز ترتیب دیئے ہیں اور انہیں کامیابی سے چلایا ہے- آپ باب کو Twitter پر **@hrbrmstr** کے ذریعے فالو کرسکتے ہیں۔

خطرات:

۱. رویّہ: بچّے انٹرنیٹ یا ورچوئل دنیا میں لوگوں سے بات چیت کرتے وقت ایسے رویّے اپنا سکتے ہیں جوکہ حقیقی دنیا میں شاید وہ کبھی بھی نہ اپنائیں۔ جسمانی طور پر غیر موجود ہونے سے بچّوں میں خصوصاً گمنامی کا شدید احساس پیدا ہوتاہے۔ بچّے اکثر ایسا رویّہ اپنانے کی طرف راغب ہوتے ہیں جن سے دوسرے بچّوں کو نقصان پہنچ سکتاہے۔ یہ سائبر بُولینگ یا گریفنگ کہلاتاہے- مزید یہ کہ آپ کے بچّے ایسے لوگوں کا نشانہ بن سکتے ہیں جو جان بُوجھ کر انہیں تنگ کرناچاہتے ہوں یا نقصان پہنچاناچاہتے ہوں۔

۲. رابطہ: بچّے اب تقریباً ہر وقت دوسروں سے بات چیت کرتے رہتے ہیں آیا ایس ایم ایس کے ذریعے، آن لائن کمیونٹیز کے ذریعے یا ورچُوئل دنیا میں گیم کھیلتے ہوئے- جسمانی طور پر غیر موجودگی کی وجہ سے بچے اکثر یہ بھول جاتے ہیں کہ جس شخص سے وہ بات کررہے ہیں وہ شاید وہ نہیں ہے جو وہ بتارہاہے یا اُس شخص کے ذہن میں اُس بچے کا بہترین مفاد نہیں ہے۔ شکاری ان ڈیجیٹل گلیوں میں پھرتے رہتے ہیں اور وہ ہر اُس طریقہ کار کو اپناتے ہیں جس کے ذریعے وہ ممکنہ شکار سے رشتہ مضبوط کرسکیں، اکثر اوقات خود اپنے آپ کو بچّہ ظاہر کرکے۔

۳. مواد: ایسے طریقوں کی کمی نہیں ہے جن کے ذریعے آپ ویڈیو، آواز، تصویر یا ٹیکسٹ پیغامات کو خود بنا کر اس کی اشاعت آن لائن کرسکتے ہیں۔ بچّوں میں اپنی اور اپنے خاندان کی معلومات کا دوسروں سے اشتراک کرنے اور حد سے زیادہ اشتراک کرنے کا لالچ بالکل حقیقی ہے اور انہیں اس بات کا احساس نہیں ہوتاہے کہ اس کا انجام کیا ہوگا۔ بچّوں سے جب کوئی شخص کسی قدم کواُٹھانے کو کہتاہے، جیسے کہ کسی لنک کو کلک کرنا، تو انہیں شاید شناخت کی چوری یا میل ویئر سے متاثر ہونے کے خطرات کا علم نہیں ہوتا۔ آخر میں یہ کہ ہم ایک ایسے زمانے میں رہ رہے ہیں جہاں جب کوئی چیز آن لائن شائع ہوجاتی ہے یا کسی سے اس کا اشتراک ہوجاتاہے تو وہ واپس

بچوں کو سائبر تحفظ کی تربیت دینا

نہیں ہوسکتی ہے۔ بچّے شاید یہ سوچیں کہ Kik, Instagram, Snapchat اور دیگر جگھوں پر اشاعتیں مختصر وقت کے لیئے نظر آتی ہیں لیکن یہ اشاعتیں آپ یا آپ کے خاندان کے کسی فرد کی زندگی میں کبھی بھی واپس آکر پریشانی کا باعث بن سکتی ہیں۔

بچوں کی آن لائن حفاظت کا بہترین طریقہ انہیں ان خطرات کے بارے میں آگاہ کرنا ہے جو انہیں لاحق ہیں اور اس بات کو یقینی بنانا ہے کہ نہ صرف آپ ان سے اس بارے میں بات کریں بلکہ وہ بھی آپ سے بات کریں۔

بچّوں کی تربیت :

سب سے پہلی چیز جو آپ اپنے بچّوں کی حفاظت کےلیئے کرسکتے ہیں وہ اُن سے بات کرنا ہے- آپ کو معلوم ہونا چاہیئے کہ آپ کے بچّے آن لائن کیا کر رہے ہیں۔ آپ انہیں آج کل کے خطرات کے بارے میں آگاہی فراہم کریں اور انہیں یہ بھی بتائیں کہ وہ کن اقدامات کے ذریعے اپنی حفاظت کرسکتے ہیں۔

۱. گھر میں حفاظت: زیادہ نقل وحرکت ہونےکے باوجود گھر ایک ایسی جگہ ہے جہاں سے محفوظ آن لائن رویّوں کی ابتداء ہوتی ہے- آپ جتنی کم عمر میں بچّوں سے اور بچّے آپ سے بات کرنا شروع کرتے ہیں اُتنا ہی بہتر ہوتاہے- آپ ان سے باقاعدگی سے آن لائن حفاظتی مسائل کے بارے میں گفتگو کریں یہاں تک کہ انہیں ایسے بُرے واقعات کے بارے میں بتائیں جو اصل میں رونما ہوچکے ہیں- اگر آپ کو نہیں پتہ کہ آپ کے بچّے کیا کررہے ہیں تو آپ اُن سے پوچھ لیں- آپ اُن سے انجان والدین بن کر جدید ترین ٹیکنالوجیز کے بارے میں بتانے کا کہیں اور ان سے پوچھیں کہ وہ اسے کیسے استعمال کرتے ہیں۔ بچّوں کو اُستاد بننے کا بہت شوق ہوتاہے، اس لئے وہ آپ سے کھل کر بات کریں گے۔ مثال کے طورپر اگر وہ Instagram پر ہیں تو اُن سے کہیں کہ وہ آپ کو اس کے استعمال کا طریقہ بتائیں، انہیں اپنے لیئے اکاؤنٹ بنانے کےلئے کہیں اور اُن کو اس پر فالو کریں- اب آپ نہ صرف بچّوں سے سیکھ رہے ہیں اور ان کی نگرانی کر رہے ہیں بلکہ اُن کے لیۓ اپنے والدین سے بات چیت کرنے میں آسانی بھی پیدا کررہے ہیں- اس کے علاوہ آپ سے جتنا ممکن ہو آپ اس بات کی یقین دہانی کرلیں کہ بچّوں کی تمام آن لائن سرگرمی گھر کے مرکزی حصے میں ہورہی ہے اور اُن کے لیئے اس کے استعمال کا وقت مقررکردیں۔ کمپیوٹر کو گھر کے مرکزی حصّے میں رکھنے سے بچّوں کے رویّے خطرناک ہونے کے امکانات کم ہوجاتے ہیں- اس کے علاوہ آپ موبائل آلات کے مرکزی چارجنگ اسٹیشنز بنانے پر غورکریں اور یہ اُصول بنا دیں کہ بچّوں کے سونے سے پہلے تمام موبائل آلات اُس میں رکھے جائیں گے۔

۲. دوسری جگھوں پر تحفظ: بچّے جب گھر سے دور ہوتے ہیں تو وہ زیادہ خطرے میں ہوتے ہیں- آپ انہیں یہ بات سمجھائیں کہ آپ کے بنائے ہوئے انٹرنیٹ کے اُصول اُن پر ہر جگہ لاگو ہوتے ہیں اور آپ اپنی پابندیوں کے بارے میں کسی بھی قابل بھروسہ شخص کو احتیاط کے ساتھ بتاسکتے ہیں- اگر اُن کے پاس موبائل آلات ہیں تو آپ ان کے استعمال کی نگرانی کریں (وقت اور بینڈ وڈتھ کے استعمال کے ذریعے) یہ دیکھنے کےلیئے کہ آیا جب وہ گھر سے دور ہوتے ہیں تو کم پابندیوں کا فائدہ تو نہیں اُٹھاتے ہیں- آپ تمام خلاف ورزیوں کو روک نہیں سکیں گے لیکن جب بھی وہ راستے سے بھٹکنے لگیں گے توآپ کے بتائے ہوئے الفاظ اُن کے ذہن میں ضرور آئیں گے-

۳. دُوسروں کے ساتھ مل کر تحفظ: آپ بچّوں پر آن لائن نظر رکھنے کے معاملے میں اکیلے نہیں ہیں بلکہ آپ کو دُوسرے والدین، سرپرستوں، بہن بھائیوں، اساتذہ، اور دوستوں سے اس معاملے میں مدد لینی چاہیئے تاکہ آپ اُن کے کسی بھی ممکنہ نقصاندہ رویّے پر نظرکھ سکیں۔

© SANS Institute 2015

بچوں کو سائبر تحفظ کی تربیت دینا

آپ اپنی کمیونٹی کو بچّوں کے ساتھ منسلک کرنے کی کوشش کریں اور بچّوں سے مثبت روابط بڑھانے پر زور دیں خصوصاً اُس وقت جب وہ دیکھیں کہ اُن کے بچے خطرناک راستے پر گامزن ہورہے ہیں۔

آخر میں یہ کہ جب بچّوں سے غلطیاں سرزد ہوجائیں توآپ ہر غلطی کو ایک تجربے کے طورپر لیں اور اُس سے سیکھنے کی کوشش کریں بجائے اس کے کہ آپ فوری تادیبی کاروائی شروع کردیں- بچّوں کو ہر دفعہ کیوں کا جواب دیں اور انہیں یاد دلائیں کہ آپ صرف انہیں ایسے خطرات سے تحفظ دلانے کی کوشش کررہے ہیں جنہیں وہ ابھی دیکھ نہیں سکتے ہیں۔ آپ انہیں یہ بتا دیں کہ جب بھی آن لائن کسی سے بات چیت کرکے انہیں کوئی غیرآرامدہ تجربہ ہو تو وہ آپ کو اس کے بارے میں بتاسکتے ہیں یا شاید وہ اس کا اسکرین شاٹ لے کر آپ کے ساتھ اُس کا اشتراک کرسکتے ہیں۔ آپ اس بات کی یقین دہانی کرلیں کہ اگر بچّوں کو اس بات کا اندازہ ہوجائے کہ اُن سے کوئی غلطی سرزد ہوگئی ہے تووہ آپ سے اُس کے بارے میں بات کرتے ہوئے آرامدہ محسوس کریں۔ آج کی ڈیجیٹل دنیا میں بچّوں کو محفوظ رکھنے کا بہترین طریقہ حقیقی دنیا کے مواصلات کے طریقوں کو کُھلا اور فعّال رکھنا ہے۔

مزید جانیئے

OUCH! کے ماہانہ سیکیورٹی تعلیم کے نیوز لیٹر کو سبسکرائب کریں،OUCH! archives تک رسائی حاصل کریں اورSANS سیکیورٹی سے مزیدآگاہی کے لئے اس ویب سائٹ کا دورہ کریں http://www.securingthehuman.org (انگریزی میں) ۔

اردو ایڈیشن

Rewterz پاکستان کی معروف انفارمیشن سکیورٹی کمپنی ہے جو پچھلے سات سالوں سے آئی ٹی سکیورٹی کے شعبے میں خدمات سرانجام دے رہی ہے - کمپنی کے بارے میں مزید معلومات کے لئے http://www.rewterz.com کا دورہ کریں یاہمارے فیس بک پیج https://www.facebook.com/Rewterz کو 'لائک' کریں یا ٹوئیٹر @Rewterz پر فالو کریں۔

وسائل:

سائبر اسمارٹ: http://www.cybersmart.gov.au/Parents.aspx

آن گارڈ آن لائن: http://www.onguardonline.gov/topics/protect-kids-online

آن لائن محفوظ رہنا: https://www.staysafeonline.org/stay-safe-online/for-parents/raising-digital-citizens

بچوں کے پینل کو محفوظ بنانا:
http://www.rsaconference.com/media/into-the-woods-protecting-our-youth-from-the-wolves-of-cyberspace

OUCH! کی ا شاعتSANS Secure The Human Programکے ذریعے ہوتی ہے اور اسے Creative Commons BY-NC-ND 4.0 License کے تحت تقسیم کرنے کی اجازت ہوتی ہے۔ آپ اس نیوز لیٹر کو تقسیم سکتے ہیں اگر آپ اس کا حوالہ دیں ، اس میں کوئی تبدیلی نہ کریں اور نہ ہی اسے تجارتی مقاصد کے لئے استعمال کریں ۔ ترجمے اور مزید معلومات کے لئےouch@securethehuman.orgپر رابطہ کریں

ایڈیٹوریل بورڈ: بل وے مین، والٹ اسکریونز، فل ہوفمن، لینس اسپٹزنر، کارمن رولی ہارڈی۔

ترجمہ: شعیب ہاشمی

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus