کمپیوٹراستعمال کرنے والوں کے لئے ماہانہ سکیورٹی تعلیم کا نیوز لیٹر

OUCH!

اس شمارے میں شامل ہے:

- جائزہ
- بنیادی اقدامات
- چھوٹے بچے

سائبر جنریشن گیپ کو محفوظ بنانا

پس منظر

ہم میں سے کئی لوگ ٹیکنالوجی کے ساتھ آرامدہ محسوس کرتے ہیں جس میں اُس کا صحیح اور محفوظ استعمال بھی شامل ہے۔ تاہم آپ کے خاندان کے دوسرے اراکین ٹیکنالوجی سے شاید اتنا آرامدہ محسوس نہیں کرتے ہوں خصوصاً اگر وہ کمپیوٹرز یا انٹرنیٹ کے دور میں بڑے نہ ہوئے ہوں۔ آپ مندرجہ ذیل اقدامات کو اپنا کر جنریشن گیپ کو محفوظ بنا سکتے ہیں۔ اس کے علاوہ یہ کہ ہو سکتا ہے کہ جو اقدامات آپ اپنے بچوں کو گھر میں محفوظ رکھنے کے لیئے اٹھاتے ہیں وہ اقدامات اُس وقت کارآمد نہیں ہوں جب آپ کے بچے کسی رشتےدار کے گھر گئے ہوئے ہوں۔ ہم آپ کو یہ بھی بتائیں گے کہ آپ اپنے بچوں کو کس طرح محفوظ آن لائن ماحول فراہم کر سکتے ہیں جب وہ رشتے داروں کے گھر جائیں۔

مہمان ایڈیٹر

برائن ہونن (Twitter **@brianhonan**) ڈبلن، آئرلینڈ میں مقیم ایک خود مختار سکیورٹی کنسلٹنٹ ہیں۔ وہ آئرلینڈ کے پہلے CERT کے بانی اور سربراہ ہیں، یوروپول کے سائبر کرائم سینٹر (EC3) کے خصوصی مشیر ہیں اور یونیورسٹی کالج ڈبلن میں انفارمیشن سکیورٹی پر لیکچر دیتے ہیں۔ انہوں نے کئی کتابیں تصنیف کی ہیں اور وہ صنعت کی کئی مطبوعات کے لیئے لکھتے ہیں۔

بنیادی اقدامات:

صرف چند بنیادی اقدامات اپنا کر کوئی بھی شخص اپنی ڈیجیٹل زندگی کو کافی حد تک محفوظ بنا سکتا ہے۔ ہم مندرجہ ذیل بیان کردہ بنیادی اقدامات کو خاندان کے کسی بھی فرد کے لیئے تجویز کرتے ہیں۔ تاہم اگر آپ کے خاندان کا کوئی فرد ان اقدامات کو نہیں سمجھتا ہے تو آپ کو ہی انہیں یہ اقدامات سمجھانے ہوں گے یا خود اُن پر عمل درآمد کرنا ہوگا۔

- **سوشل انجینئرنگ**: آپ آسان الفاظ میں سوشل انجینئرنگ کی اصطلاح کو اس طرح بیان کریں تاکہ اُسے کوئی بھی سمجھ سکے۔ اس قسم کے حملے نئے نہیں ہیں کیونکہ دھوکے باز اور مجرم فنکار ہزاروں سالوں سے موجود ہیں۔ اب فرق صرف اتنا ہے کہ برے لوگ اب ان طریقوں کا اطلاق انٹرنیٹ پر کر رہے ہیں۔ آپ آج کل سب سے زیادہ دھوکہ دہی کے طریقوں کی مثال دیں جیسے کہ سب سے زیادہ استعمال ہونے والی فشنگ ای میلز یا مائیکروسافٹ کی مشہور ٹیکنیکل سپورٹ کی فون کالز۔ اگر کچھ اور نہیں تو آپ کم از کم اس بات کو یقینی بنائیں کہ آپ کے خاندان کے افراد اس بات کو سمجھیں کہ وہ کبھی بھی اپنے کمپیوٹر کا پاس ورڈ یا ریموٹ ایکسس کسی اور کو نہیں دیں۔ آخر میں یہ کہ آپ اس بات کو یقینی بنائیں کہ اگر آپ کے خاندان کے افراد کبھی بھی اس معاملے میں غیر آرامداہ محسوس کر رہے ہوں یا اُن کے پاس کچھ سوالات ہوں جیسے کہ کسی نے انہیں ای میل یا کال کی ہے کسی معلومات کے سلسلے میں تو وہ اس صورتِ حال میں کوئی بھی قدم اُٹھانے سے پہلے آپ سے بات کر لیں۔
- **گھر کا وآئی-فائی نیٹ ورک**: آپ اس بات کو یقینی بنائیں کہ آپ کے گھر کا وآئی-فائی نیٹ ورک محفوظ ہے۔ کم از کم اس بات کو یقینی بنائیں کہ ڈیفالٹ ایڈمنسٹریٹر کا پاس ورڈ تبدیل ہو گیا ہو، گھر کے وآئی-فائی تک رسائی حاصل کرنے کے لیئے ایک مضبوط پاس ورڈ درکار ہو اور نیٹ ورک کنیکشن میں تازہ ترین اینکرپشن کا استعمال ہو رہا ہو۔ آپ اپنے وآئی-فائی کو اس طرح کنفگر کرنے پر غور

سائبر جنریشن گیپ کو محفوظ بنانا

بُزرگوں کو اپنے گھر میں موجود ٹیکنالوجی کی حفاظت کرنے اور مہمان بچوں کو محفوظ ماحول فراہم کرنے میں آپ کی مدد کی ضرورت پڑ سکتی ہے۔

کریں کہ وہ محفوظ DNS، جیسے کہ www.opendns.org کا استعمال کرے۔ اس طرح کی محفوظ DNS سروس نہ صرف لوگوں کو متاثرہ ویب سائٹس پر جانے سے روک سکتی ہیں بلکہ آپ کو یہ اختیار بھی دیتی ہیں کہ آپ لوگوں کو کن ویب سائٹس پر جانے دیتے ہیں اور کن ویب سائٹس تک ان کی رسائی روکتے ہیں۔ یہ طریقہ خصوصاً گھر آئے مہمان بچوں کے لیئے بہت سودمند ہے۔

- **پیچنگ**: اپنے سسٹم کو جدید ترین اور اپڈیٹ رکھنا، کسی بھی ٹیکنالوجی کو محفوظ بنانے کے اُن بنیادی طریقوں میں سے ایک ہے جسے آپ اپنا سکتے ہیں- اس بات کو یقینی بنائیں کے گھر کے تمام آلات (بشمول موبائل آلات) اور ایپلیکیشنز پوری طرح پیچڈ ہیں۔ اس چیز کو یقنی بنانے کے لیئے سب سے آسان ترین طریقہ آٹومیٹک اپڈیٹ کو فعال کرنا ہے۔
- **اینٹی وائرس**: لوگ کئی دفعہ ایسی چیزوں کو انسٹال یا اُن پر کلک کرنے کی غلطی کر دیتے ہیں جو انہیں نہیں کرنا چاہیئے۔ اینٹی وائرس جب کہ تمام میلویئر کو روک نہیں سکتا ہے، یہ عام حملوں کی نشاندہی اور انہیں روکنے میں مدد ضرور فراہم کرتا ہے۔ اس لیئے آپ اس بات کی یقین دہانی کر لیں کہ آپ کے گھر کے تمام کمپیوٹرز میں اینٹی وائرس انسٹال، فعال اور تازہ ترین ہے۔
- **پاس ورڈ**: مضبوط پاس ورڈ تمام آلات اور آن لائن اکاؤنٹس کو محفوظ رکھنے کا سب سے اہم ذریعہ ہے۔ آپ اپنے خاندان کے افراد کو مضبوط پاس ورڈ بنانے کا طریقہ بتائیں۔ اس سلسلے میں اُن کے لیئے پاس فریز کا استعمال اور اُسے یاد رکھنا آسان ترین طریقہ ہو سکتا ہے۔ ایک اور طریقہ پاس ورڈ مینیجر کو انسٹال کرنا اور خاندان کے افراد کو اُس کے استعمال کے بارے میں تعلیم دینا ہے۔ اگر یہ طریقہ کارآمد نہیں ہے تو آپ انہیں پاس ورڈ کو ایسی محفوظ جگہ پر لکھنا اور زخیرہ کرنا سکھا دیں جس تک رسائی صرف اُن کو ہی حاصل ہو۔ کسی بھی اہم آن لائن اکاؤنٹ کے لیئے آپ ٹو اسٹیپ ویریفیکیشن کا استعمال کر سکتے ہیں۔
- **بیک اپس**: جب سارے طریقے ناکام ہو جائیں تو بیک اپس آپ کی زندگی آسان کر دیتے ہیں۔ آپ اس بات کو یقینی بنائیں کہ آپ کے خاندان کے افراد کے پاس سادہ اور قابلِ بھروسہ فائل بیک اپ سسٹم موجود ہے۔

آپ کو ماہانہ یا ہر سہ ماہی پر اس بات کو یقینی بنانا ہے کہ اوپر بیان کردہ تمام تجاویز صحیح طور پر لاگو ہیں۔ بدترین صورتِ حال میں آپ ریموٹ ایڈمنسٹریٹو سافٹ ویئر کو کسی آلہ پر انسٹال کرنے کے لیئے غور کریں۔ تاہم اگر آپ یہ قدم اُٹھاتے ہیں تو آپ اس بات کو یقینی بنائیں کہ یہ اِنکرپٹ ہے، اور مضبوط اور منفرد پاس ورڈ کے ذریعے محفوظ ہے۔

مہمان بچے:

اکثر اوقات جب بچے کسی رشتے دار کے گھر جاتے ہیں، جیسے کہ دادا/دادی کے گھر، تو جن قوانین کا اطلاق آپ نے اپنے گھر میں کر رکھا ہے، ہو سکتا ہے کہ وہ یہاں مؤثر نہ ہوں۔ اس میں وہ قوانین بھی شامل ہیں جو آپ نے اپنے بچوں کی آن لائن حفاظت کے لیئے بنائے ہیں۔ آپ مندرجہ ذیل اقدامات اُٹھا کر بچوں کی حفاظت کر سکتے ہیں۔

سائبر جنریشن گیپ کو محفوظ بنانا

قوانین: آپ اس بات کی یقین دہانی کر لیں کہ اگر آپ کی اپنے بچّوں کی حفاظت کے لیئے کچھ قوانین یا توقّعات ہیں تو آپ کے رشتےداروں کو اُن کا علم ہونا چاہیئے۔ مثال کے طور پر، کیا کوئی ایسا قانون ہے کہ بچے کتنی دیر تک آن لائن گیم کھیل سکتے ہیں یا اپنے موبائل آلات تک کب رسائی حاصل کر سکتے ہیں؟ آپ ہم پر بھروسہ کریں جب ہم آپ کو یہ کہتے ہیں کہ آپ اس خام خیالی میں نہ رہیں کہ آپ کے بچے ان قوانین کے بارے میں اپنے دادا/دادی یا خاندان کے دوسرے افراد کو بتائیں گے۔ ایک طریقہ یہ ہے کہ آپ قوانین کی فہرست بنائیں اور اُس کا اشتراک اُن رشتےداروں کے ساتھ کریں جن کے ہاں آپ کے بچے زیادہ جاتے ہیں۔

کنٹرول: اگر آپ کے بچے ٹیکنالوجی کو اپنے سرپرستوں سے بہتر طور پر سمجھتے ہیں تہ ہو سکتا ہے کہ وہ اس کا فائدہ اُٹھائیں۔ مثال کے طور پر، بچے اپنے دادا/دادی کے کمپیوٹر میں ایڈمنسٹریٹو رائٹس مانگ سکتے ہیں جس کے بعد وہ اپنی مرضی سے کچھ بھی کر سکتے ہیں جیسے کہ کوئی ایسی گیم انسٹال کرنا جسے آپ نہیں چاہتے ہیں کہ وہ کھیلیں۔ آپ اس بات کی یقین دہانی کرلیں کہ آپ کے رشتےدار اس بات کو سمجھیں کہ وہ آپ کے بچوں کو اُن کے طےشدہ کنٹرولز سے زیادہ کنٹرولز فراہم نہیں کریں۔

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:

سوشل انجینیئرنگ: http://www.securingthehuman.org/ouch/2014#november2014
گھر کے نیٹ ورک کو محفوظ کرنا: http://www.securingthehuman.org/ouch/2014#january2014
پاس فریزز: http://www.securingthehuman.org/ouch/2015#april2015
اینٹی وائیرس: http://www.securingthehuman.org/ouch/2014#december2014
اپنے بچوں کی آن لائن حفاظت کرنا: http://www.securingthehuman.org/ouch/2013#april2013
ٹیکنیکل فون سپورٹ کے دھوکے: http://www.onguardonline.gov/articles/0346-tech-support-scams
سائبر سکیور ہوم کا پوسٹر بنانا: http://www.securingthehuman.org/resources/posters

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

ترجمہ: شعیب ہاشمی