کمپیوٹر استعمال کرنے والوں کے لئے ماہانہ سکیورٹی تعلیم کا نیوز لیٹر

OUCH!

اس شمارے میں شامل ہے:

- جائزہ
- اپنے آپ کو محفو ظ رکھنا
- اپنے کمپیوٹر/اکاؤنٹ کو محفوظ بنانا
- والدین کے لیئے ہدایات

محفو ظ اور بحفاظت طریقے سے گیمنگ کرنا

جائزہ

آن لائن گیمنگ تفریح کا ایک عمدہ طریقہ ہے تا ہم اس کے ساتھ کچھ منفرد خطرات بھی لاحق ہیں۔ نیوز لیٹر کے اس شما رے میں ہم اُن اقدامات پر نظر ڈالیں گے جن کے ذریعے آپ اپنی اور اپنے خاندان کی آن لائن گیمنگ کے دوران حفاظت کرسکتے ہیں ۔

مہمان ایڈیٹر

جیک ولیمز رینڈیشن انفوسیک کے بانی اور پرنسپل کنسلٹنٹ، SANS کے سند یافتہ انسٹرکٹر اور SANS کے کئی کورسز کے شریک مصنف ہیں۔ وہ ٹوئیٹر پر **@MalwareJake** کے ذریعے فعال ہیں اور **malwarejake.blogspot.com** پر باقاعدگی سے بلاگ کرتے ہیں۔

اپنے آپ کو محفوظ رکھنا

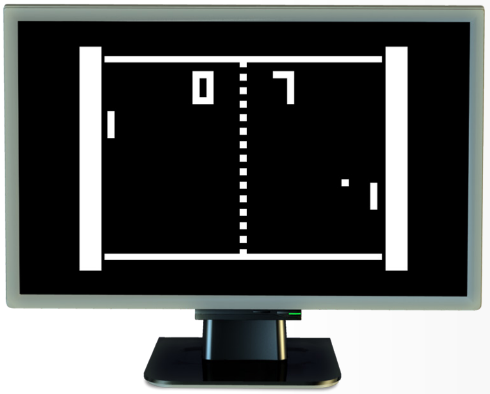
آن لائن گیمنگ کوجو چیز زیادہ دلفریب بناتی ہے وہ یہ ہے کہ آپ اسے دنیا میں کسی بھی جگہ بیٹھے ہوئے کسی بھی شخص کے ساتھ کھیل سکتے ہیں اور بات چیت کر سکتے ہیں- اکثر آپ شاید ان لوگو ں کو جانتے بھی نہیں ہیں جن لوگوں کے سا تھ آپ کھیل رہے ہوتے ہیں۔ ویسے تو لوگوں کی اکثریت آپ کی طرح تفریح کے لیئے آن لائن ہوتی ہے لیکن کچھ لوگ ایسے بھی ہوتے ہیں جو نقصان پہنچانا چاہتے ہیں- آپ کو اپنے آپ کو محفوظ رکھنے کےلیئے مندرجہ ذیل اقدامات اپنانے چاہیئں۔

- آپ کسی بھی ایسے پیغام سے محتاط رہیں جو آپ کو کوئی قدم اٹھانے کا کہے جیسے کہ کسی لنک پر کلک کرنا یا کوئی فائل ڈاؤن لوڈ کرنا- فشنگ حملوں کی طرح، برے لوگ بھی آپ کو بیوقوف بنا کر یا دھوکہ دہی کے ذریعے ایسے اقداما ت اٹھانے پر مجبور کر دیتے ہیں جن کے ذریعے آپ کا کمپیوٹر میلویئر سے متاثر ہوجا تا ہے- اگر کو ئی پیغام آپ کو عجیب لگے، بہت زیادہ ضروری لگے یا پھر سچ نہیں لگ رہا ہو تو آپ متنبہ ہو جائیں کیوںکہ شاید یہ حملہ ہو سکتا ہے۔
- کئی آن لائن گیمز کی اپنی مالیاتی منڈیاں ہوتی ہیں جہاں آپ تجارت کرسکتے ہیں، اشیاء کا تبادلہ کر سکتے ہیں یا خیالی (ورچوئل) اشیاء بھی خرید سکتے ہیں- بالکل حقیقی دنیا کی طرح، ان سسٹمز پر بھی دھوکے باز ہوتے ہیں جو دھوکہ دہی کے ذریعے آپ سے پیسے نکلوانے یا اُسے چرانے کی کوشش کرتے ہیں۔
- اصل پیسوں کے ذریعے کسی بھی گیم میں شامل اشیاء کا لین دین کرتے ہوئے آپ ہمیشہ محتاط رہیں- آ پ یہ لین دین صرف شہرت یافتہ اور جانی پہچانی مارکیٹ پلیس کے ذریعے کریں۔
- آ پ اور آپ کے بچّے اپنی معلومات کا انٹرنیٹ پر محدود اشتراک کریں۔ آپ کبھی بھی اپنی تفصیلی ذاتی معلومات، جیسے کہ آپ کا پاس ورڈ یا گھر کا پتہ، کا اشتراک نہیں کریں۔
- کئی ویب سائٹس، جیسے کہ آن لائن بینکنگ کی ویب سائٹ، آپ کی شناخت کی تصدیق کے لیئے سکیورٹی سوال کا استعمال کرتی ہیں- حملہ آور ان سکیورٹی سوالات کا جواب حاصل کرنے کے لیئے اپنے شکار سے آن لائن گیمز کے ذریعے دوستی کرتے ہیں۔ یاد رکھیں کہ آپ گیم کھیلنے کے دوران لوگوں کے پوچھے گئے کسی بھی سوال کا جواب دینے کے پابند نہیں ہیں۔

محفوظ اور بحفاظت طریقے سے گیمنگ کرنا

اپنے سسٹمز/اکاؤنٹس کو محفوظ بنانا

اگلا قدم آپ کا اپنے کمپیوٹر کو محفوظ بنانا ہے- برے لوگ آپ کے کمپیوٹر یا گیمنگ اکاؤنٹ پر قبضہ کرنے کی کوشش کریں گے اس لیئے آپ کو ان کی حفاظت کرنی ہے۔



آن لائن گیمنگ کے دوران اپنے آپ کو محفوظ رکھنے کیلئے موثر ترین طریقوں میں مضبوط پاس ورڈز کا استعمال کرنا، اپنے کمپیوٹر کو محفوظ بنانا اور اجنبی لوگوں سے بات کرتے ہوئے جب عجیب پیغامات آئیں تو عقل کا استعمال کرنا شامل ہے۔

- آپ اپنے کمپیوٹر اور کسی بھی گیمنگ اکاؤنٹ کے لیئے مضبوط پا س ورڈ کا استعمال کریں- اس طرح حملہ آور آپ کے پاس ورڈ کا با آسانی اندازہ نہیں لگا سکیں گے اور نہ ہی آپ کے اکاؤنٹس پر قبضہ کر سکیں گے- اگر آپ کی گیم ٹو-اسٹیپ ویریفیکیشن کی سہولت مہیا کرتی ہے تو آپ اس کا استعمال کریں- اس کے علاوہ آپ اس بات کی یقین دہانی کرلیں کہ آپ کے ہر گیمنگ اکاؤنٹ کا پاس ورڈ مختلف ہے- اس طرح اگر آپ کے کسی ایک اکاؤنٹ کا پاس ورڈ چوری ہو جاتا ہے تو باقی اکاؤنٹس محفوظ رہتے ہیں۔
- آپ جدید ترین آپریٹنگ سسٹم اور گیمنگ سافٹ ویئر کا استعمال کرکے اپنے کمپیوٹر کو محفوظ بنا سکتے ہیں- آپ کے آپریٹنگ سسٹمز اور ویب براؤزرز کی طرح پرانے اور فرسودہ گیمنگ سافٹ ویئر میں بھی کئی معروف کمزوریاں ہوتی ہیں جن کا فائدہ اٹھاتے ہوئے حملہ آور آپ کے کمپیوٹر کو ہیک کر سکتے ہیں- اپنے کمپیوٹر اور گیمنگ ایپلیکیشن کو اپڈیٹ کرنے سے آپ معروف کمزوریوں کے خطرات کو کم کر دیتے ہیں۔
- اینٹی وائیرس کا استعمال کریں اور اس بات کی تاکید کر لیں کہ وہ اپڈیٹڈ ہے اور کسی بھی فائل جسے آپ کھولتے ہیں اسے فوراً اسکین کر دیتا ہے۔
- گیمنگ سافٹ ویئر کو صرف قابل بھروسہ ویب سائٹس سے ڈاؤن لوڈ کریں۔ اگر آپ گیم کھیلنے کے لیئے کوئی سافٹ ویئر استعمال کر رہے ہیں تو اس بات کی تاکید کر لیں کہ آپ اسے اس گیم کے وینڈر کی ویب سائٹ یا کسی اور قابل بھروسہ ویب سائٹ سے ڈاؤن لوڈ کر رہے ہیں۔ اکثر سائبر حملہ آور گیم کا جعلی یا متاثرہ ورژن بناتے ہیں اور پھر اسے اپنے سرور کے ذریعے تقسیم کر دیتے ہیں- اگر آپ ان ورژنز میں سے کوئی انسٹال کرتے ہیں تو برے لوگوں کو آپ کے کمپیوٹر پر مکمل اختیار حاصل ہو جاتا ہے۔
- گیمنگ کے ایڈ-آن پیکس، جو کہ اکثر گیمنگ کمیونیٹی خود بناتی ہے، کا گیم میں نئی خصوصیات کو شامل کرنے کیلئے کثرت سے استعمال ہوتا ہے- حملہ آور کبھی کبھی ان گیمنگ پیکس کو میلویئر سے متاثر کر دیتے ہیں جس کا پتہ لگانا اینٹی وائیرس کیلئے بہت دشوار ہو سکتا ہے۔ گیمز کی طرح آپ ایڈ-آنز کو بھی قابل بھروسہ جگہوں سے ڈاؤن لوڈ کریں- اس کے علاوہ یہ کہ اگر کوئی ایڈ-آن آپ کو اینٹی وائیرس کو غیر فعال کرنے کا کہے یا فائروال میں کچھ تبدیلیاں کرنے کا کہے تو آپ اسے استعمال نہیں کریں۔
- غیر قانونی (انڈرگراؤنڈ) مارکیٹس نے دھوکہ دہی (چیٹنگ) کی سرگرمیوں کی کھل کر حمایت کی ہے۔ غیر اخلاقی ہونے کے علاوہ کئی دھوکہ دہی والے پروگرامز خود بھی روٹ کٹس ہوتے ہیں جو کہ خود ایک خطرناک ترین میل ویئر ہے- آپ کبھی بھی گیم میں دھوکہ دہی والے سافٹ ویئرز انسٹال نہیں کریں۔
- آپ جس بھی گیمنگ سافٹ ویئر کو انسٹال کر رہے ہیں اس کی ویب سائٹ کی جانچ پڑتال کر لیں- کئی گیمنگ ویب سائٹس میں ایک علیحدہ سیکشن ہوتا ہے جو آپ کو اپنے آپ اور اپنے کمپیوٹر کو محفوظ بنانے کیلئے مشورے فراہم کر تا ہے- آپ اس بات کی تاکید کر لیں کہ آپ ان کے بتائے گئے مشوروں پر عمل کریں گے۔

محفوظ اور بحفاظت طریقے سے گیمنگ کرنا

- آخر میں یہ کہ آپ اپنے موبائل آلات پر گیم کھیلتے ہوئے بھی اتنا ہی مہتات رہیں جتنا آپ اپنے کمپیٹر پر کھیلتے ہوئے ہوتے ہیں- سائبر حملہ آور اب موبائل آلات کو بھی نشانہ بنانا شروع ہو گئے ہیں۔

والدین کیلئے ہدایت

اگر آپ والدین میں سے ہیں تو اس بات کی تاکید کر لیں کہ آپ کے بچے اوپر بتائی گئی ہدایت پر عمل کر رہے ہیں (اگر بچے چھوٹے ہیں تو آپ کو خود ان کیلئے یہ اقدامات کرنے ہوں گے)- اس کے علاوہ آپ اپنے بچوں کو خود خطرات سے آگاہ کریں- تعلیم اور بات چیت اپنے بچوں کو محفوظ رکھنے کےلیئے موثر طریقے ہیں۔ بچوں سے بات شروع کرنے کیلئے ہمارا پسندیدہ طریقہ بچوں سے یہ پوچھنا ہے کہ ان کی گیمز کیسے چلتی ہیں- آپ اُن کو اپنی آن لائن دنیا دکھانے دیں اور یہ بتانے دیں کہ یہ گیم کیسے کھیلتے ہیں۔ ویسے آپ ان کے ساتھ گیم کھیل بھی سکتے ہیں- اس کے علاوہ آپ اُن کو اُن لوگوں کے بارے میں بتانے کا کہیں جن سے وہ آن لائن ملتے ہیں۔ اکثر اوقات آن لائن گیمنگ آپ کے بچے کی سماجی زندگی کا بڑا حصہ ہو سکتی ہیں- بچوں سے بات چیت کے ذریعے (اُن کی حوصلہ افزائی کریں کہ وہ آپ سے بات کریں)آپ کسی بھی مسئلے کی نشان دہی کر سکتے ہیں اور انھیں ٹیکنالوجی سے کہیں ذیادہ تحفظ فراہم کر سکتے ہیں۔

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

فشنگ حملے: http://www.securingthehuman.org/ouch/2013#february2013

پاس ورڈز: http://www.securingthehuman.org/ouch/2013#october2013

اینٹی وائیرس کیا ہے؟: http://www.securingthehuman.org/ouch/2014#december2014

آن لائن محفوظ رہیں: http://www.staysafeonline.org/stay-safe-online/for-parents/gaming-tips

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