تمام لوگوں کے لیئے ماہانہ سکیورٹی آگاہی کا نیوزلیٹر

OUCH!

اس شمارے میں شامل ہے:

- اپنے آپ کو محفوظ بنانا
- اپنے کمپیوٹر کو محفوظ بنانا
- والدین کے لیئے تجاویز

محفوظ طریقے سے آن لائن گیم کھیلنا

جائزہ

آن لائن گیمنگ تفریح کا ایک بہت بڑا ذریعہ ہے، تاہم اس کے ساتھ کُچھ مخصُوص خطرات بھی لاحق ہیں- اس نیوز لیٹر میں ہم ان نُکات پر بات کریں گے جن کے ذریعے آپ اپنے آپ اور اپنے خاندان کی گیمنگ کے دوران حفاظت کر سکتے ہیں-

مہمان ایڈیٹر

اِسٹیوآرمسٹرانگ ،لاجیکلی سکیور، کے بانی، SANS کے سند یافتہ انسٹرکٹر اور CyberCPR، جو کہ ایک انسیڈنٹ مینیجمنٹ پلیٹ فارم ہے، کے آرکیٹیکٹ ہیں- وہ ٹوئیٹر پر **@Nebulator** کے ذریعے فعّال ہیں اور کئی بڑی گیمنگ کی تنظیموں کے ساتھ کام کرتے ہیں جو کہ اُن کے بچپن اور پیشہ ورانہ زندگی کا ایک خواب تھا-

اپنے آپ کو محفوظ بنانا

جو چیز آن لائن گیمنگ کو تفریح کا باعث بناتی ہے وہ یہ ہے کہ آپ اس کے ذریعے دنیا میں کسی کے ساتھ کہیں سے بھی گیم کھیل سکتے ہیں اور بات چیت کر سکتے ہیں- اکثر آپ کو یہ بھی پتہ نہیں چلتا کہ آپ کس کے ساتھ گیم کھیل رہے ہیں- حالانکہ لوگوں کی اکثریت آپ کی طرح آن لائن تفریح کی غرض سے آتی ہے لیکن کُچھ ایسے بھی لوگ ہوتے ہیں جو دُوسروں کو نُقصان پہنچانے کی غرض سے آتے ہیں- آن لائن گیمنگ کے دوران حفاظت کے لیئے آپ مُندرجہ ذیل اقدامات اُٹھائیں-

- آپ کسی بھی ایسے پیغام کے بارے میں مُحتاط رہیں جو آپ کو کوئی کام کرنے پر اُکسائے، جیسے کسی لِنک پر کِلک کرنا یا کسی فائل کو ڈاؤن لوڈ کرنا- بالکل ای میل فِشنگ حملوں کی طرح بُرے لوگ آپ کو آن لائن گیمز میں بھی بیوقوف بنانے کی کوشش کریں گے یا دھوکہ دہی کے ذریعے کُچھ ایسے کام کرنے کو کہیں گے جن کے ذریعے آپ کا کمپیوٹر مُتاثر ہو جائے یا وہ آپ کی شناخت چُرا لیں- اگر آپ کو کوئی پیغام عجیب لگ رہا ہو، بہت عُجلت میں لگ رہا ہو یا وہ ناقابلِ یقین لگ رہا ہو تو آپ مشکوک ہو جائیں کیونکہ یہ ایک حملہ ہو سکتا ہے-
- کئی آن لائن گیمز کی اپنی ‹فائیننشل مارکیٹس› ہوتی ہیں جہاں آپ تجارت کر سکتے ہیں، بارٹر کر سکتے ہیں یا شاید ورچُوئل اشیاء خرید سکتے ہیں- بالکل حقیقی دنیا کی طرح اِن سِسٹمز میں بھی دھوکے باز ہوتے ہیں جو کہ دھوکہ دہی کے ذریعے آپ کے جمع کیئے ہوئے پیسے یا ورچُوئل کرنسی چُرانے کی کوشش کرتے ہیں- آپ صرف اُن لوگوں سے لین دین کریں جنہوں نے اپنی قابل بھروسہ ساخت قائم کی ہوئی ہو-
- اپنے کسی بھی گیمنگ اکاؤنٹ کے لیئے مضبوط پاس فریز استعمال کریں- اس طرح حملہ آور آپ کے اکاؤنٹس کے پاس ورڈز کا اندازہ نہیں لگا سکتے ہیں اور نہ ہی اُس تک رسائی حاصل کر سکتے ہیں- اگر آپ کی گیم ٹُواسٹیپ ویریفیکشن کی سہولت فراہم کر رہی ہے تو آپ اُس کا استعمال کریں- مزید یہ کہ آپ اس بات کی یقین دہانی کر لیں کہ آپ کے تمام آن لائن اکاؤنٹس کے پاس ورڈز ایک دُوسرے سے مختلف ہیں- اس طرح اگر ایک گیم کی رسائی کسی حملہ آور تک ہو بھی جاتی ہے تو باقی تمام اکاؤنٹس محفوظ رہتے ہیں- کیا آپ اپنے تمام پاس ورڈز یاد نہیں رکھ سکتے ہیں؟ اس صورت میں آپ پاس ورڈ مینیجر کے استعمال پر غور کریں-

اپنے کمپیوٹر کو محفوظ بنانا

بُرے لوگ آپ کے گیمنگ والے کمپیوٹر کو ہیک کرنے کی کوشش کر سکتے ہیں- آپ مُندرجہ ذیل اقدامات اٹھا کر اپنے کمپیوٹر کو محفوظ بنا سکتے ہیں-

محفوظ طریقے سے آن لائن گیم کھیلنا

- اپنے کمپیوٹر پر آپ جدید ترین آپریٹنگ سسٹم اور گیمنگ سافٹ ویئر کا ورژن چلا کر اُسے محفوظ بنائیں- پُرانے اور فرسُودہ سافٹ ویئر میں جانی پہچانی کمزوریاں ہوتی ہیں جن کا فائدہ اٹھا کر حملہ آور آپ کے کمپیوٹر کو ہیک کر سکتے ہیں- اپنے کمپیوٹر اور گیمنگ ایپلیکیشنز کو اپڈیٹ رکھ کر آپ زیادہ تر خطرات سے بچ جاتے ہیں-
- آپ اینٹی وائرس کا استعمال کریں اور اس بات کی یقین دہانی کر لیں کہ وہ اپڈیٹ ہے اور آپ کے کسی بھی فائل کے کھولنے پر اُس کی اُسی وقت جانچ پڑتال کرتا ہے-
- گیمنگ سافٹ ویئر کو صرف قابل بھروسہ ویب سائٹس سے ڈاؤن لوڈ کریں- بسا اوقات سائبر حملہ آور گیم کے جعلی یا مُتاثرہ ورژن بناتے ہیں اور پھر اُنہیں اپنے سرور کے ذریعے تقسیم کرتے ہیں-
- گیمنگ ‹ایڈ-آن› پیکس، جو کہ کمیونیٹی خود بناتی ہے، بہت کثرت سے نئی خُصوصیات شامل کرنے کے لیئے استعمال ہوتی ہیں- حملہ آور کبھی کبھی ان گیمنگ پیکس کو میلویئر کے ذریعے مُتاثر کر دیتے ہیں- بالکل اسی طرح جس طرح آپ گیمز کو ڈاؤن لوڈ کرتے ہیں، اس بات کو یقینی بنائیں کہ آپ ‹ایڈ-آنز› کو بھی قابل بھروسہ جگہوں سے ڈاؤن لوڈ کریں- مزید یہ کہ اگر کوئی ایڈ آن آپ کو اپنے اینٹی وائرس کو غیر فعّال کرنے کا کہے یا آپ کی سکیورٹی سیٹینگز میں کوئی تبدیلی کرے تو آپ اُسے استعمال نہیں کریں-
- انڈرگراؤنڈ مارکیٹس دھوکہ دہی (چیٹنگ) کی سرگرمی کی حمایت میں کافی پیش پیش ہیں- غیر اخلاقی ہونے کے ساتھ ساتھ کئی دھوکہ دہی کے پروگرامز بذات خود میلویئر ہوتے ہیں جو کہ آپ کے کمپیوٹر کو مُتاثر کر دیتے ہیں- آپ کبھی بھی دھوکہ دہی والے سافٹ ویئر یا ویب سائٹس کا استعمال نہیں کریں-
- آپ جو بھی آن لائن گیمنگ سافٹ ویئر استعمال کر رہے ہیں، اس کی ویب سائٹ کا ضرور دورہ کریں- کئی گیمنگ ویب سائٹس میں ایک مخصُوص حصّہ ہوتا ہے جو آپ کو یہ بتاتا ہے کہ آپ کو اپنے آپ کو اور اپنے سسٹم کو کیسے محفوظ بنانا ہے-
- آخر میں یہ کہ آپ اپنے موبائل آلات میں گیمز کھیلتے ہوئے اتنا ہی ہوشیار رہیں جتنا آپ اپنے کمپیوٹر پر کھیلتے ہوئے ہوتے ہیں- سائبر مجرمان اب موبائل آلات کو بھی ہدف بنا رہے ہیں-

محفوظ طریقے سے آن لائن گیمنگ کرنے کے لیئے مضبوط پاس ورڈز کا استعمال کرنا چاہیئے، اپنے کمپیوٹر کی حفاظت کرنی چاہیئے اور کسی بھی عجیب پیغام یا گزارش کی صورت میں عام فہم کا استعمال کرنا چاہیئے-

والدین اور سرپرستوں کے لیئے تجاویز

جب بچے آن لائن گیم کھیل رہے ہوتے ہیں تو انہیں اضافی حفاظت اور تعلیم کی ضرورت ہوتی ہے- اپنے بچوں کی حفاظت کے لیئے اہم ترین اقدامات میں تعلیم اور ان سے کھلی بات چیت شامل ہے- بچوں سے بات چیت کے لیئے ہماری پسندیدہ چالوں میں سے ایک یہ ہے کہ آپ ان سے پوچھیں کہ ان کی گیمز کیسے کھیلتے ہیں، انہیں اپنی آن لائن دنیا کی سیر کرانے دیں اور یہ دکھانے دیں کہ ایک مخصُوص گیم کیسے چلتی ہے- اگر ہو سکے تو آپ ان کے ساتھ گیم کھیل کر بھی دیکھیں- اس کے علاوہ آپ انہیں ان لوگوں کے بارے میں بھی بتانے دیں جن سے وہ آن لائن ملتے ہیں- اکثر اوقات آن لائن گیمنگ آپ کے بچے کی سماجی زندگی کا ایک بڑا حصّہ ہو سکتی ہے- بچوں سے بات کر کے (اور بچوں سے باتیں اگلوا کر) آپ کسی بھی مسلے کی نشاندہی کر سکتے ہیں اور ٹیکنالوجی کے مقابلے میں کہیں زیادہ بہتر طریقے سے حفاظت فراہم کر سکتے ہیں- مزید اقدامات میں شامل ہے:

محفوظ طریقے سے آن لائن گیم کھیلنا

- آپ کو پتہ ہونا چاہیئے کہ بچے کون سی گیمز کھیل رہے ہیں اور اس بات کی یقین دہانی کر لینی چاہیئے کہ وہ گیمز اُن کی عُمر کے لحاظ سے موزوں ہے۔
- آپ اپنے بچّوں کے آن لائن معلومات کے اشتراک کو محدود کر دیں۔ مثال کے طور پر اُنہیں کبھی بھی اپنے پاس ورڈ، عُمر، فون نمبر یا گھر کے پتہ کا اشتراک نہیں کرنے دیں۔
- آپ گیمنگ کمپیوٹر کو کسی ایسی کُھلی جگہ پر رکھیں جہاں آپ اُس پر نظر رکھ سکیں۔ مزید یہ کہ چھوٹے بچّوں کو اپنے کمروں میں یا رات کو دیر تک گیم کھیلنے کی اجازت نہیں دیں۔
- بدمعاشی، بُری زبان کا استعمال یا دوسرے غیر سماجی رویّے ایک مسئلہ ہو سکتے ہیں۔ آپ اپنے بچّوں پر نظر رکھیں، اگر وہ گیم کھیلنے کے بعد کُچھ پریشان دکھائی دیتے ہیں تو ہو سکتا ہے کہ وہ آن لائن کسی کی بدمعاشی کا شکار ہوئے ہوں۔ اگر ایسا ہے تو آپ اُنہیں وہ گیم کھیلنے سے روکیں اور اُنہیں بچّوں کے دوستانہ ماحول میں کھیلنے کا کہیں یا اُنہیں صرف اُن دوستوں کے ساتھ آن لائن گیمز کھیلنے کا کہیں جو قابلِ بھروسہ ہوں۔
- آپ بچّوں کی گیمز میں ‹اِن اپپ› خریداری کی حمایت کے بارے میں معلومات حاصل کریں اور یہ بھی کہ وہ گیمز کس قسم کے پیرینٹل اوورائیڈ فراہم کرتی ہیں۔

مزید جانیئے

OUCH! کے ماہانہ سیکیورٹی تعلیم کے نیوز لیٹر کو سبسکرائب کریں، OUCH! archives تک رسائی حاصل کریں اور SANS سیکیورٹی سے مزید آگاہی کے لئے اس ویب سائٹ کا دورہ کریں securingthehuman.sans.org/ouch/archives (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:

گھر کے نیٹ ورک کو محفوظ بنانا:	https://securingthehuman.sans.org/ouch/2016#february2016
سوشل انجینئرنگ:	https://securingthehuman.sans.org/ouch/2017#january2017
پاس فریزز:	https://securingthehuman.sans.org/ouch/2017#april2017
پاس ورڈ مینیجر:	https://securingthehuman.sans.org/ouch/2015#october2015
ٹو اسٹیپ ویریفیکیشن:	https://securingthehuman.sans.org/ouch/2015#september2015

ایڈیٹوریل بورڈ: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley۔

ترجمہ: شعیب ہاشمی