کمپیوٹراستعمال کرنے والوں کے لئے ماہانہ سکیورٹی تعلیم کا نیوز لیٹر

OUCH!

اس شمارے میں شامل ہے:

- جائزہ
- پرائیویسی
- سکیورٹی

سوشل میڈیا

جائزہ:

سوشل میڈیا ویب سائٹس جیسے کہ facebook, twitter, instagram, linkedin, بہت زبردست وسائل ہیں جن کے ذریعے آپ دنیا بھر کے لوگوں سے مل سکتے ہیں ،ان سے بات چیت کر سکتے ہیں اور معلومات کا اشتراک کر سکتے ہیں۔ تاہم ان تمام سہولیات کے ساتھ کچھ خطرات بھی لاحق ہیں جو کہ نہ صرف آپ تک مہدود ہیں بلکہ آپ کے خاندان، احباب اور آجر کو بھی لاحق ہیں۔ اس نیوزلیٹر میں ہم ان خطرات کے بارے میں بتائیں گے اور یہ بھی بتائیں گے کہ ان سائٹس کو محفوظ طریقے سے کیسے استعمال کرنا ہے۔

مہمان ایڈیٹر

تانیہ بیکم کافی پرانی سکیورٹی کنسلٹنٹ ہیں۔ وہ ایک دہائی سے زیادہ عرصے سے SANS کے ساتھ مصنفہ اور انسٹرکٹر کے طور پر منسلک ہیں جن میں SEC502, SEC542, SEC401, MGT414, AUD507 اور کئی دوسرے کورسز شامل ہیں۔ آپ انہیںtwitter پر **@tbaccam** کے ذریعے فالو کر سکتے ہیں۔

پرائیویسی:

سوشل میڈیا میں ایک عام تشویش اپنی معلومات کی حفاظت کرناہے۔ ممکنہ خطرات میں شامل ہے:

- **اپنے مستقبل پر اثر انداز ہونا**: کچھ تنظیمیں سوشل میڈیا سائٹس کو لوگوں کا پس منظر جانچنے کے لیئے استعمال کرتی ہیں۔ شرمندگی کا باعث بننے والی تصاویر یا پوسٹس، چاہے جتنی پرانی ہو جائیں، آپ کی نوکری ہونے یا ترقی پانے سے روک سکتی ہیں۔ اس ک علاوہ کئی جامعات بھی نئے طلبہ کی درخواست پر ایسی جانچ پڑ تال کرتی ہیں۔ پرائیویسی کے اختیارات آپ کو محفوظ نہیں کر سکتے ہیں کیونکہ یہ تنظیمیں آپ کواپنے اُن پیجز یا کچھ پوسٹس کو «لائک» یا «جوان» کرنے کا کہ سکتی ہیں جو کہ مختلف سائٹس پر آرکائیو ہو ری ہوں۔
- **آپ پر حملے**: سائبر حملہ آور آپ کی پوسٹس کا تجزیہ کر سکتے ہیں اور ان کو استعمال کر کے آ پ یا آپ کی تنظیم کی معلومات تک رسائی حاصل کر سکتے ہیں۔ مثال کے طور پر وہ آپ کی اشتراک کردہ معلومات کو آپ کے " خفیہ سوالات " کے جوابات کا اندازہ لگانے کے لیئے استعمال کر سکتے ہیں تاکہ آپ کے آن لائن پاس ورڈز کو ری-سیٹ کر سکیں، مخصوص ای-میل کے ذریعے ہدف بنائیں، جو کہ ‹اسپیئرفشنگ› کہلاتا ہے، یا وہ آ پ کی تنظیم میں کسی کو آپ کے طور پر کال کر سکتے ہیں۔ اس کے علاوہ یہ حملے حقیقی دنیا میں بھی اثرانداز ہو سکتے ہیں جیسے کہ آپ کے گھر اور کام کی جگہ کی نشاندی کرنا۔
- **غیر دانستہ طور پر اپنے آجر کو نقصان پہنچانا**: مجرمان یا آپ کے حریف، آپ کی اپنی تنظیم کے خلاف شائع کردہ کسی بھی حساس معلومات کو آپ کے آجر کے خلاف استعمال کر سکتے ہیں۔ مزید یہ کہ آپ کی پوسٹ ممکنہ طور پر آپ کی تنظیم کی ساکھ خراب کر سکتی ہے۔ اپنی ملازمت سے متعلق کوئی بھی چیز شائع کرنے سے پہلے آپ اس بات کا یقین کر لیں کہ آپ نے اپنی تنظیم کی متعلقہ پالیسیز پڑھ لی ہیں۔ اس کے علاوہ یہ کہ آپ کی کچھ سوشل میڈیا پوسٹس کی نگرانی بھی کی جا سکتی ہے۔

سب سے بہترین تحفظ یہ ہے کہ آپ اپنی پوسٹس کو محدود کردیں۔ یہ صحیح ہے کہ پرائیویسی کے اختیارات کسی حد تک تحفظ فراہم کرتے ہیں تاہم یہ اکثر مبہم ہوتے ہیں اور آپ کے علم میں لائے بغیر تبدیل بھی ہوتے رہتے ہیں۔ آپ جس پوسٹ کو پرائیویٹ سمجھتے ہیں وہ جلد ہی کسی بھی وجہ سے پبلک ہو سکتی ہے۔ اس کے علاوہ یہ کہ آپ کی پوسٹ کی پرائیویسی اتنی ہی محفوظ ہے جتنا کہ وہ لوگ، جن کے ساتھ

سوشل میڈیا

آپ اس کا اشتراک کر رہے ہیں۔ آپ جتنے زیادہ لوگوں یا دوستوں کے ساتھ کسی معلومات کا اشتراک کریں گے اتنا ہی زیادہ اس کے عوامی ہونے کا امکان بڑھ جائے گا۔ آپ کو کسی بھی معلومات کے اشتراک کے وقت یہ بات ذہن میں رکھنی چاہیئے کہ وہ معلومات عوامی ہوسکتی ہیں یا ہو جائیں گی اور انٹرنیٹ کا مستقل حصہ بن جائیں گی۔

آخر میں یہ کہ آپ اس بات سے بھی محتاط رہیں کہ آپ کے دوست آپ کی کون سی معلومات کا اشتراک کر رہے ہیں۔ اگر وہ کسی ایسی چیز کا اشتراک کر رہے ہیں جس سے آپ غیرآرامدہ محسوس کر رہے ہیں تو آپ ان سے اس کو ہٹانے کا مطالبہ کریں۔ اگر وہ اسے ہٹانے سے انکار کر دیں یا نظرانداز کر دیں توآپ اس سوشل میڈیا سائٹ سے رابطہ کریں اور انہیں اس مواد کو ہٹانے کا کہیں۔ اسی طرح آپ بھی دوسروں کے بارے میں کچھ بھی شائع کرتے وقت بااحترام رہیں۔

سوشل میڈیا سائٹس بہت پُرلطف اور طاقتور ہوتی ہیں لیکن آپ کو کسی کے ساتھ کچھ بھی اشتراک کرتے وقت محتاط رہنا چاہیئے۔

سکیورٹی:

پرائیویسی خدشات کے علاوہ آپ مندرجہ ذیل اقدامات اپنا کر اپنے سوشل میڈیا اکاؤنٹس اور آن لائن سرگرمیوں کو محفوظ بنا سکتے ہیں:

- **لاگ-ان**: آپ اپنے ہر اکاؤنٹ کو مضبوط اور منفرد پاسورڈ کے ذریعے محفوظ بنائیں اور اس کا اشتراک کسی کے ساتھ نہ کریں۔ مزید یہ کہ کئی سوشل میڈیا سائٹس مضبوط اوتھنٹیکیشن کی حمایت کرتی ہیں جیسے کہ ٹو-اسٹیپ ویریفیکیشن۔ جب بھی ممکن ہو آپ ہمیشہ ان مضبوط اوتھنٹیکیشن کے طریقوں کو فعال کر دیں۔ آخر میں یہ کہ آپ اپنے سوشل میڈیا اکاؤنٹ کو کسی دوسری ویب سائیٹ پر لاگ-ان کرنے کے لئے استعمال نہیں کریں، کیونکہ اگر وہ اکاؤنٹ ہیک ہو گیا تو پھر آپ کے باقی تمام اکاؤنٹس بھی غیر محفوظ ہو جائیں گے۔
- **پرائیویسی سیٹنگز**: اگر آپ پرائیویسی سیٹنگز کا استعمال کرتے ہیں تو اس بات کا یقین کر لیں کہ آپ باقاعدگی سے اس کا جائزہ لیتے رہیں اور اسے جانچتے رہیں۔ سوشل میڈیا سائٹس اکثر پرائیویسی سیٹنگز کو تبدیل کر دیتی ہیں، اس لیئے غلطی کے امکانات بڑھ جاتے ہیں۔ اس کے علاوہ کئی ایپلیکیشنز اور سروسز آپ کو اپنی پوسٹ کے ساتھ محل وقوع شامل کرنے کی سہولت فراہم کرتی ہیں (جو کہ جیو ٹیگنگ کہلاتی ہے)۔ اگر آپ اپنے محل وقوع کو نجی رکھنا چاہتے ہیں تو باقاعدگی سے ان سیٹنگز کی جانچ کرتے رہیں۔
- **انکرپشن**: سوشل میڈیا سائیٹس، ویب سائٹ سے آپ کے کنکشن کو محفوظ بنانے کے لئے ایک انکرپشن، HTTPS، کا استعمال کرتی ہیں۔ کچھ ویب سائٹس جیسے کہ+ twitter, google میں یہ پہلے سے ہی فعال ہوتا ہے جب کہ دوسری ویب سائٹس میں آپ کو خود HTTPS کو فعال کرنا پڑتا ہے۔ آپ اپنے سوشل میڈیا کے اکاؤنٹ کی سیٹنگز کا جائزہ لیں اور جب بھی ممکن ہو،HTTPS کو ڈیفالٹ کنیکشن کے طور پر فعال کر دیں۔
- **ای میل**: آپ ان ای-میلز کے بارے میں مشکوک رہیں جو یہ دعویٰ کرتی ہیں کہ وہ سوشل میڈیا کی سائٹ کی طرف سے ہیں کیونکہ یہ سائبر مجرمان کی طرف سے اسپوف حملے ہو سکتے ہیں۔ اس طرح کے پیغامات کا جواب دینے کا سب سے محفوظ طریقہ یہ ہے کہ آپ براہ راست سوشل میڈیا کی ویب سائیٹ پر لاگن کریں، شاید پہلے سے محفوظ بک مارک کے ذریعے، اور پھر اس ویب سائیٹ کے ذریعے کسی بھی پیغام یا نوٹیفیکیشن کو پڑھیں یا اس کا جواب دیں۔
- **مضر لنکس/اسکیمز**: آپ سوشل میڈیا سائٹس پر مشکوک لنکس یا ممکنہ اسکیمز کے بارے میں محتاط رہیں۔ برے لوگ سوشل میڈیا کے ذریعے اپنے حملے کرتے ہیں۔ صرف اس لیئے کہ کوئی پیغام آپ کے دوست کی طرف سے شائع کیا گیا ہے، اس کا یہ مطلب

سوشل میڈیا

نہیں ہے کہ وہ اصل میں اس کی طرف سے آیا ہو، ہو سکتا ہے کہ اس کا اکاؤنٹ ہیک ہو گیا ہو۔ اگر آپ کے خاندان کے کسی فرد یا دوست نے کوئی ایسا عجیب پیغام بھیجا ہے جس کی آپ تصدیق نہیں کر سکتے ہیں (جیسے کہ وہ لٹ گئے ہیں اور انھیں پیسوں کی ضرورت ہے) تو آپ انھیں ان کے موبائل پر کال کریں یا کسی اور ذریعے سے رابطہ کریں اور اس بات کا تصدیق کریں کہ وہ پیغام حقیقت میں ان کی طرف سے ہی ہے۔

- **موبائل اپلیکیشنز**: زیادہ تر سوشل میڈیا سائٹس آپ کو موبائل اپلیکیشنز کے ذریعے آن لائن اکاؤنٹس تک رسائی فراہم کرتی ہیں۔ آپ اس بات کی یقین دہانی کر لیں کہ آپ ان موبائل اپلیکیشنز کو با اعتماد سائٹس کے ذریعے ڈاؤن لوڈ کریں اور اس بات کی بھی کہ آپ کا اسمارٹ فون مضبوط پاس ورڈ کے ذریعے محفوظ ہے۔ اگر آپ کا اسمارٹ فون ‹ان-لاک› ہے اور وہ کھو گیا ہے تو کوئی بھی اس اسمارٹ فون کے ذریعے آپ کی سوشل میڈیا سائٹس تک رسائی حاصل کر سکتا ہے اور آپ کے طور پر کچھ بھی شائع کر سکتا ہے۔

سوشل میڈیا سائٹس دنیا بھر سے رابطے کا ایک حیرت انگیز ذریعہ ہیں- اگر آپ اوپر دی گئی تجاویز پر عمل کرتے ہیں تو آپ اپنے آن لائن تجربے کو کافی حد تک محفوظ بنا سکتے ہیں۔ سوشل میڈیا سائٹس کے محفوظ استعمال یا کسی ‹ان-آتھرائزڈ› سرگرمی کے بارے میں مزید جاننے کے لیئے آپ اپنی سوشل میڈیا سائٹ کے سکیورٹی پیج کا دورہ 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:

پاس فریزز:	http://www.securingthehuman.org/ouch/2015#april2015
ٹوُ اسٹیپ ویریفیکیشن:	http://www.securingthehuman.org/ouch/2013#august2013
موبائل ایپلیکیشنز کا محفوظ طریقے سے استعمال:	http://www.securingthehuman.org/ouch/2015#january2015
بچّوں کو سائبر تحفظ کی تربیت دینا:	http://www.securingthehuman.org/ouch/2015#june2015
فیس بک سکیورٹی:	https://www.facebook.com/safety

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