کمپیوٹراستعمال کرنے والوں کے لئے ماہانہ سیکیورٹی تعلیم کا نیوز لیٹر

OUCH!

اس شمارے میں شامل ہے:

- آپ کی معلومات
- اپنی ڈیوائیس کو وائپ کرنا
- سم /بیرونی اسٹوریج کارڈ

اپنی موبائل ڈیوائیس کوتلف کرنا

جائزہ:

موبائل ڈیوائیسز جیسے کہ اسمارٹ فونز اور ٹیبلیٹس، میں جددت اور ترقی حیرت انگیز طور پر جاری ہے جسکے نتیجے میں ہم میں سے کئی لوگ اکثر ہر اٹھارہ مہینوں میں اپنی موبائل ڈیوائیس تبدیل کر لیتے ہیں- بدقسمتی سے کئی لوگ اپنی پرانی موبائل ڈیوائیسز کو یہ سوچ بغیر کہ ان میں کتنی زیادہ ذاتی معلومات جمع ہو چکی ہیں، تلف کر دیتے ہیں۔ اس شمارے میں ہم اپنی توجہ اس بات پر مرکروز رکھیں گے کہ کتنی طرح کی ذاتی معلومات آپکے موبائل میں ہو سکتی ہیں اور آپ اسے کس طرح تلف کرنے سے پہلے محفوظ طریقے سے وائپ کرسکتے ہیں۔

اگر آپ کی موبائل ڈیوائیس آپکے آجر کی جانب سے جاری کی گئی ہے یا اس پر تنظیم سے متعلق معلومات محفوظ ہیں تو آپ مندرجہ ذیل اقدامات کو اپنانے سے پہلے اپنے سُپروائزر سے اُس ڈیوائیس کے باقاعدہ بیک اپ اور تلف کرنے کے طریقہ کار کے بارے میں پتہ کرلیں۔

مہمان ایڈیٹر

کرسٹو فر کراؤلی (@CCrowMontance; +ChrisCrowley)واشنگٹن ڈی سی میں مقیم ایک کنسلٹنٹ ہیں ۔ وہ SANSانسٹیٹیوٹ میں موبائل ڈیوائس سیکیورٹی اینڈ ایتھیکل ہیکنگ (SEC575)کے معروف انسٹرکٹر ہیں اور انسیڈنٹ رسپونس ٹیم مینجمنٹ (MGT535)کے مصنف ہیں۔

آپ کی ذاتی معلومات :

موبائل ڈیوائیسز آپ کی سوچ سے کہیں زیادہ ذاتی معلومات محفوظ کرتی ہیں شاید آپکے کمپیوٹر سے بھی زیادہ۔ ایک موبائل ڈیوائیس میں محفوظ مخصوص معلومات میں شامل ہوسکتا ہے:

- آپ کہاں رہتے ہیں، کہاں کام کرتے ہیں اور کن جگہوں کا زیادہ کثرت سے دورہ کرتے ہیں۔
- آپ کی ایڈرس بُک میں موجود تمام کانٹیکٹس کی تفصیلات بشمول آپکے خاندان، دوست اور ساتھ کام کرنے والے لوگ۔
- کال ہسٹری بشمول آنے والی، جانے والی اور مسڈ کالز۔
- ٹیکسٹ اور آواز پیغامات۔
- ایپلیکیشنز جیسے کہ گیمز اور سوشل میڈیا ایپلیکیشنز کے اندرچیٹ سیشنز۔
- مقام کی ہسٹری پر مبنی جی ۔ پی ۔ ایس کوآرڈینیٹس یا سیل ٹاور۔
- انٹر نیٹ براؤزنگ کی ہسٹری، کوکیز اورCached پیجز۔
- ذاتی تصاویر، ویڈیوز، آڈیو ریکارڈنگ اور ای میل۔
- پہلے سےمحفوظ پاس ورڈز اور ذاتی اکاؤنٹس تک رسائی جیسے کہ آپ کا آن لائن بینک یا ای میل۔
- کلاؤڈ پر محفوظ تصاویر، فائلز یا معلومات تک رسائی۔
- صحت سے متعلق معلومات جس میں آپکے دل کی دھڑکن کی رفتار، بلڈ پریشر یا ڈائٹ شامل ہے۔

اپنی موبائل ڈیوائیس کوتلف کرنا

اپنی ڈیوائیس کو وائپ کرنا:

جیسا کہ آپ دیکھ سکتے ہیں کہ آپ کے موبائل ڈیوائیس پر کافی زیادہ حساس معلومات موجود ہوسکتی ہیں۔ اس بات سے قطعہ نظر کہ آپ اپنا موبائل کیسے تلف کرتے ہیں جیسےکہ اسے عطیہ کردیتے ہیں، خاندان کے کسی دوسرے فرد کودے دیتے ہیں یا چاہے اسے پھینک دیتے ہیں، آپ کو پہلے اس بات کی تاکید کرنی چاہیئے کہ آپ نے اس میں موجود تمام حساس معلومات مٹا دی ہیں۔ اس کے علاوہ اگر آپ اپنی موبائل ڈیوائیس کو واپس کر رہے ہیں یا اس کے بدلے نئی ڈیوائیس لے رہے ہیں تو اس صورت میں بھی آپ کو اپنی معلومات مٹانے کی ضرورت ہے۔ اگر آپ یہ نہیں کریں گے تو جس کسی کے پاس بھی آپ کی موبائل ڈیوائیس جائے گی وہ باآسانی آپ کی معلومات تک رسائی حاصل کرسکتا ہے۔ البتہ اپنی معلومات کو وائپ کرنے سے پہلے آپ کو اس کا بیک اپ لینے کی ضرورت ہوگی۔ ان معلومات میں تصاویر، ویڈیوزیا کوئی بھی دوسری معلومات شامل ہوسکتی ہیں۔ ایک بار آپ اپنی ڈیوائیس کو وائپ کردیں تو پھر آپ اُس میں موجود کسی بھی معلومات کو دوبارہ ریکئور نہیں کرسکتے ہیں۔

آپ اپنے موبائل ڈیوائس کو تلف کرتے وقت اس بات کا دیہان رکھیں کہ آپ نے اس میں فیکٹری سیٹینگز لاگو کردی ہیں اور اس میں سے سم یا ایس۔ڈی کارڈ نکال لیا ہے۔

ایک دفعہ آپ اپنی معلومات کا بیک اپ لے لیں تو پھر آپ اسے محفوظ طریقے سے ڈیلیٹ کرسکتے ہیں۔ فائلز، تصاویر یا معلومات کو صرف ڈیلیٹ کرنا ناکافی ہوگا۔ صرف ڈیلیٹ کی ہوئی معلومات انٹر نیٹ پر موجود مفت ٹولز کے ذریعے باآسانی ریکئور ہوسکتی ہیں۔ اس کے بجائے آپ کو اپنی ڈیوائیس پر موجود تمام معلومات کو محفوظ طریقے سے ڈیلیٹ کرنا چاہیئے، اس طریقے کو وائپنگ کہتے ہیں۔ یہ اصل میں معلومات کو اوور رائٹ کردیتا ہے جس سے اس بات کی تاکید ہوجاتی ہے کہ یہ معلومات ریکئور نہیں ہوسکتی ہیں۔ یہ کرنے کا سب سے آسان طریقہ اپنی ڈیوائیس کی "فیکٹری سیٹنگز" کا استعمال کرنا ہے۔ یہ آپ کی ڈیوائیس کو واپس اُس حالت میں لے جائے گا جس میں آپ نے اسے پہلے خریدا تھا۔ ہم اس نتیجے پر پہنچتے ہیں کہ فیکٹری سیٹنگز سب سے محفوظ اور آسان ترین طریقہ ہے اپنی موبائل ڈیوائیس سے معلومات کو نکالنے کا- فیکٹری ریسیٹ کا فنکشن مختلف ڈیوائیسز میں الگ ہوتا ہے۔ تین سب سے مشہور ڈیوائیسز کے طریقہ کار درجہ ذیل ہیں:

- ایپل iOSڈیوائیسز: Settings | General | Reset | Erase All Content and Settings
- اینڈروائڈ ڈیوائیسز: Settings | Privacy | Factory Data Reset
- ونڈوز فونز: ـ Settings | About | Reset Your Phone

اگر آپ کے پاس ابھی بھی فیکٹری سیٹنگز سے متعلق سوالات ہیں تو آپ اپنی ڈیوائیس کا 'مین-ول' یا مینوفیکچرر کی ویب سائٹ دیکھ سکتے ہیں۔

سم اور بیرونی کارڈز:

آپ کی معلومات کا آپ کی ڈیوائیس پر ذخیرہ ہونے کے علاوہ آپ کو اس بات کو بھی مدِ نظر رکھنا ہے کہ آپ کو اپنی سم (Subscriber Identity Module) کارڈ کا کیا کرنا ہے۔ سم کارڈ کے ذریعے ہی آپ کی ڈیوائیس سیلولر فون یا ڈیٹا سے کنیکشن بناتی ہے۔ جب آپ اپنی ڈیوائس میں فیکٹری ریسیٹ کرتے ہیں تو سم کارڈ آپ کے اکاؤنٹ کی معلومات کو برقرار رکھتا ہے۔ اگر آپ اپنا موبائل نمبر وہی رکھ رہے ہیں اور کسی دوسری ڈیوائیس

اپنی موبائل ڈیوائیس کوتلف کرنا

پر منتقل ہورہے ہیں تو آپ کو چاہیئےکہ فون بیچنے والے شخص سے اپنی سم کارڈ منتقل کرنے کے بارے میں بات کریں- اگر یہ ممکن نہیں ہے جیساکہ مثال کے طور پر اگر آپ کا نیا فون مختلف سائز کی سم استعمال کرتا ہے تو آپ کو چاہیئےکہ آپ اپنی پرانی سم کو اُٹھائیں اور اسے خود ٹکڑے ٹکڑے کردیں یا اسے ضائع کردیں تاکہ کوئی اور اسے استعمال نہیں کرسکے۔

آخر میں یہ کہ کچھ موبائل ڈیوائیسز مزید اسٹوریج حاصل کرنے کےلئے علیحدہ SD (Secure Digital)کارڈ کا استعمال کرتی ہیں- ان اسٹوریج کارڈز میں اکثر تصاویر، اسمارٹ فون کی ایپلیکیشنز اور دوسری حساس معلومات شامل ہوتی ہیں۔ یاد رہے کہ آپ اپنی موبائل ڈیوائیس کو تلف کرنے سے پہلے اس میں سے بیرونی اسٹوریج کارڈ کو نکال لیں (کچھ ڈیوائیسز میں ایس۔ڈی کارڈ بیٹری کے خانے میں چھپا ہوتا ہے، ممکنہ طور پر بیٹری کے نیچ)۔ یہ کارڈز اکثر دوسری موبائل ڈیوائیسز میں بھی استعمال ہوسکتے ہیں۔ اگر اپنے ایس۔ڈی کارڈ کو دوبارہ استعمال کرنا ممکن نہ ہوتو ہمارا مشورہ یہ ہے کہ آپ اسے اپنی سم کارڈ کی طرح خود تلف کریں۔

اگر آپ اس نیوز لیٹر میں بتائے گئے اقدامات سے مطمئن نہیں ہیں تو آپ اپنی موبائل ڈیوائیس کو، جس اسٹور سے آپ نے خریدا تھا، وہاں لے جائیں اور تربیت یافتہ ٹیکنیشن سے مدد حاصل کریں۔ آخر میں یہ کہ اگر آپ اپنی ڈیوائیس پھینکنے جارہے ہیں تو ہمارا مشورہ یہ ہے کہ آپ اسے کسی کو عطیہ کرنے کے بارے میں سوچیں۔ بہت ساری بہترین خیراتی تنظیمیں استعمال شدہ موبائل ڈیوائیسز قبول کرتی ہیں۔

مزید جانئے:

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 سایٹ کا دورہ کریںhttp://www.securingthehuman.org(انگریزی میں) ۔

اردو ایڈیشن

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

وسائل:

NIST SP800-88 Rev. 1: http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf

OUCH!: سپا کیپ: http://www.securingthehuman.org/ouch/2013#september2013

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

ترجمہ: شعیب ہاشمی